Ministero dell' Istruzione, dell' Università e della Ricerca
Istituto Comprensivo Statale "ALESSANDRO VOLTA"
Infanzia - Primaria - Secondaria I Grado
Via Volta, 13 - 20093 Cologno Monzese (MI) Tel. 02 25492649
Fax: 02 25492650 Cod. Mecc. MIIC8EH003 - C.F. 97632210155
E-mail:*miic8eh003@istruzione.it* PEC: *miic8eh003@pec.istruzione.it*
Fatturazione Elettronica Codice Univoco : **UFR9XA**
Sito Web dell'istituto: www.scuolavolta.gov.it

E-Safety Policy

Politica adottata dall'Istituto Comprensivo *Alessandro Volta* in materia di prevenzione e gestione dei rischi nell'uso delle TIC.

1.Introduzione

- Scopo della e-safety policy

La Policy di e-safety è un documento programmatico autoprodotto dalla Scuola volto a descrivere: la visione dell'uso e del ruolo delle tecnologie informatiche, le norme comportamentali e le procedure per l'utilizzo delle TIC (**T**ecnologie dell'**I**nformatica e della **C**omunicazione) in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.
Pertanto, scopo del presente documento è quello di informare l'utenza per un *uso corretto e responsabile delle apparecchiature informatiche* collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.
In particolare, l'intento della Scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche", ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.
Gli utenti, siano essi maggiorenni o 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.

Ruoli e Responsabilità ovvero 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 all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

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;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

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) Alunni

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.

1) 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.
- 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.

2) 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 gli alunni 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.

3) 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;

- 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, 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 dell'alunno.
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 verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario/libretto delle comunicazioni;
- 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 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 degli alunni 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 e dai 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.

La policy si integra con il **REGOLAMENTO DI ISTITUTO** quanto a norme comportamentali relative all'uso delle dotazioni tecnologiche della Scuola, della rete wifi e del traffico internet e dei Laboratori informatici.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti

"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.

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

Il corpo docente ha partecipato e partecipa a corsi di formazione anche nell'ambito del Piano Nazionale Scuola Digitale, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate nella rete dell'ambito di appartenenza e possiede generalmente una discreta base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. E' inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.
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; può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali appositamente create, corsi di aggiornamento online.

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

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

Sul sito web della scuola (www.scuolavolta.gov.it) sarà possibile trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri

con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati come il sito "Generazioni connesse", ecc.

- 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 sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate. 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 si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.
- Accesso a internet: filtri, antivirus e sulla navigazione.

L'accesso a internet è possibile e consentito per la didattica nei laboratori multimediali e nelle aule dotate di LIM. Solo il docente dalla propria postazione può consentire agli alunni di accedere a internet. Le postazioni non sono dotate di webcam. L'accesso è per tutti 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, secondo le impostazioni date dall'Animatore digitale che periodicamente provvede alla manutenzione e aggiornamento del sistema informatico dei laboratori, ove necessario richiedendo l'intervento di tecnici esterni. Le postazioni degli alunni (client) sono occasionalmente utilizzate anche dai docenti, quando questi si servono dei laboratori. I docenti hanno piena autonomia nel collegamento ai siti web.

- Gestione accessi (password, backup, ecc.)

L'accesso al sistema informatico per la didattica, server e internet, nei laboratori multimediali è consentito al personale docente attraverso l'assegnazione di una password.
La password è comune e consente di accedere alla rete e non al server. I docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. 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

In ottemperanza a quanto richiesto dal MIUR e dal Ministero per la semplificazione e la Pubblica Amministrazione, in materia di digitalizzazione e informatizzazione della PA, e al fine ottimizzare il servizio scolastico ed assicurare modalità di rapporto corrette ed efficaci all'interno dell'Istituto, tutto il personale in servizio presso l'IC Volta di Cologno Monzese è provveduto è fornito di un indirizzo personale di posta elettronica.
Verificato che l'estensione dell'indirizzo cognome.nome@scuolavolta.gov.it utilizzato dall'istituto è compatibile con le norme sulla privacy, tutto il personale dovrà utilizzare la propria casella per la gestione della corrispondenza interna.
La casella personale di posta elettronica è costituita dal cognome e nome seguito da @scuolavolta.gov.it

Tutte le comunicazioni, gli avvisi, le convocazioni, le circolari interne ecc. sono inviati tramite e-mail alla casella di posta istituzionale in oggetto.
Tutte le comunicazioni, gli avvisi e le circolari divulgati tramite sito web o inviati per posta elettronica si intendono regolarmente notificati a tutto il personale.
Le circolari/avvisi segnalati come urgenti che comportano presa visione/adesione ad personam ed eventuale riscontro in Segreteria saranno trasmesse e divulgate anche con modalità diverse.
Si invita pertanto tutto il personale ad effettuare giornalmente l'accesso alla posta e consultare il sito web www.scuolavolta.gov.it.

REGOLAMENTO SULL'USO DELLA POSTA ELETTRONICA ISTITUZIONALE:

La casella di posta elettronica assegnata a ciascun dipendente è uno strumento di lavoro. Coloro i quali sono assegnatari di una o più caselle di posta elettronica sono pertanto responsabili del loro corretto utilizzo.
La casella di posta elettronica istituzionale sarà:

- utilizzata per tutti gli scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo da un solo utente.
- L'Istituto fa comunque esplicito divieto a tutti gli utenti di:
- utilizzare le caselle di posta elettronica istituzionale (@scuolavolta.gov.it) per acquisti on line.
- Inviare a dar corso a catene telematiche di messaggi (c.d. "Catene di Sant'Antonio")

In caso di cessazione del rapporto di lavoro, o per qualsivoglia ragione, l'Amministratore del Sistema provvederà a disattivare l'indirizzo di posta elettronica. Per problematiche relative all'account, all'accesso o all'uso della posta rivolgersi in Segreteria.

-Uso delle *Google Apps for Education*

L'Istituto Comprensivo "A. Volta" di Cologno Monzese ha attivato le Applicazioni ***Google Apps for Education***, ora rinominate Google Suite, l'obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, la circolazione delle informazioni interne e pian piano cercare di creare uno "spazio didattico intermedio" dove insegnanti e alunni possono collaborare, scambiare materiali, tenere memoria, comunicare in tempo reale, in modo sincrono e asincrono, sia in classe sia da "casa". Un "cloud" di Istituto raggiungibile e praticabile con qualsiasi strumento che sia connesso ad internet e fruibile da "dovunque tu sia" organizzato con Applicazioni dedicate (es. ***GoogleClassroom***) e non (es, Gruppi – Sites - Drive ecc.). Le applicazioni Google consentono la gestione di documenti personali (documenti di testo, fogli elettronici, presentazioni) che sono anche condivisibili. Le ***Google Apps for Education*** garantiscono sicurezza e privacy, connessione e interoperabilità, comunicazione facilitata tra docenti e con gli studenti. ***Google Apps*** include decine di funzioni di sicurezza progettate specificatamente per mantenere i dati al sicuro, protetti e sotto controllo. I dati appartengono solo all'utente e gli strumenti di ***Google Apps*** consentono di controllarli e di stabilire con chi e in che modo condividerli. Un esempio: agli alunni della scuola secondaria è stata creata una casella di posta elettronica "a norma" e legale; essi, tuttavia, possono comunicare solo gli utenti del dominio @scuolavolta.gov.it del nostro istituto a garanzia di un uso "interno" della stessa. La casella postale è liberamente utilizzabile all'interno del dominio. In caso di trasferimento ad altra scuola,essa sarà disabilitata entro un mese dal trasferimento (il personale o i ragazzi trasferiti saranno avvisati per tempo della disattivazione in modo da poter salvare i propri messaggi e documenti). Nello specifico della posta elettronica dell'Istituto Comprensivo "A. Volta" l'Amministratore dei servizi ***Google Apps for Education*** (attualmente corrispondente al Dirigente Scolastico) dichiara di operare con le seguenti modalità:

- crea gli account e le caselle di posta per gli utenti e genera le credenziali per il primo accesso;

- gestisce i gruppi e relativi account collettivi (ad esempio docenti, plessi ecc.);
- NON PUO' accedere alle caselle di posta degli utenti, né ad altri dati personali degli utenti contenuti nelle altre Google Apps (Calendari, Sites - Google Drive, etc.), salvo che tali informazioni non siano condivise dall'utente stesso;
- può modificare le credenziali di accesso di un utente SOLO su richiesta esplicita dell'utente stesso (ad esempio se l'utente non riesce più ad accedere al proprio account);
- non è in possesso delle password di accesso al sistema dei singoli utenti. Le password iniziali, dopo la trasmissione agli utenti, vengono distrutte;
- può visualizzare statistiche sull'utilizzo del sistema (ad esempio: data dell'ultimo accesso o spazio utilizzato).

- Blog e sito web della scuola

La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati sotto la supervisione del Dirigente scolastico, che valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.
Il Dirigente Scolastico ha nominato un Responsabile dell'accessibilità.
Il Blog http://bibliovolta.blogspot.it/?m=1-page/ accessibile dal sito della scuola è gestito dall'Amministratore 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). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

5. Prevenzione, rilevazione e gestione dei casi

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 dello smartphone, dei pc dellascuola collegati alla rete.
Il telefono cellulare o lo smartphone non sono richiesti dalla scuola, perché non sono ritenuti indispensabili in ambito scolastico, ma vengono forniti dai genitori degli alunni soprattutto per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. 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, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a internet.

- Azioni

Le azioni previste di 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, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore;
- 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

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 di 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 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.

- 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 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 a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

Gestione dei casi

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

Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione dei bambini, 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 o degli adulti.
I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dall'adulto e pertanto luogo di "complicità" e di piccole "trasgressioni", di scambi "confidenziali"condivisi fra gli amici nella rete o con il cellulare.
Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gestione dei casi di "prepotenza" o "prevaricazione"

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

Il bullismo si esplica, infatti, con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto o 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 email 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, presente in ogni normale intenzione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).
In considerazione dell'età degli alunni considerati, possono prefigurarsi alcune forme di interazione 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 ruolo molto significativo nel ridurre la dimensione del fenomeno.
Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe e anche d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving.
Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.
Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire nei bambini un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza"ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.
Inoltre, la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

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 è comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino 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.

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.

- Procedure operative per la gestione dei casi.

LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali;
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;

- Non inviare a nessuno fotografie tue o di tuoi amici;
- Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso;
- Chiedi sempre al tuo 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 o uno scherzo può rivelarsi offensivo per qualcun altro;
- Non rispondere alle offese ed agli insulti;
- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Se ricevi materiale offensivo (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 rispondere; riferisci anche 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 di classe o ai tuoi genitori prima di inviare messaggi da casa;
- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo 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.

LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
- Discutete con gli 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;
- 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 policy e-safety 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.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

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: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo;
- Partecipate alle esperienze on-line: navigate insieme a vostro figlio, incontrate gli amici on-line, discutete degli 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 vedono immagini particolari o se ricevono 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 e 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.

Consigli in base all'età

Se tuo figlio 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 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'e-mail di tuo figlio dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni. Se tuo figlio vuole usare IM verifica che i suoi contatti siano limitati agli amici conosciuti. Specifica che non può inserire nuovi contatti senza averti prima consultato.
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, modalità di utilizzo di IM (messaggistica istantanea). 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 salone o in una stanza accessibile a tutta la famiglia e non nella camera di tuo figlio ALMENO fino ai **16 anni**.

Il presente documento è approvato con delibera dal Collegio dei Docenti e dal Consiglio di Istituto.