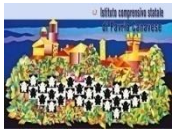

Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO STATALE
Piazza della Repubblica 6 - 10083 FAVRIA tel. 0124 470067
e-mail: TOIC865006@istruzione.it **- sito web.** www.icfavria.gov.it
CF 85502080014 - C.M. TOIC865006

E-SAFETY POLICY – IC FAVRIA

SCOPO E FINALITA'

Il presente documento è volto a regolamentare i comportamenti nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica , in ambito scolastico e anche extra-scolastico, relativamente alle attività di compiti assegnati a casa .

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 acquisir 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 .

SEZIONE 1

RUOLI E RESPONSABILITA'

1. **IL DIRIGENTE SCOLASTICO**

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

- Garantire 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 e delle differenze , un utilizzo positivo e responsabile delle TIC
- Garantire l'esistenza di un sistema in grado di consentire il monitoraggio ed il controllo interno della sicurezza on line

- 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 , COLLABORATORE DEL DS , RESPONSABILE DEL LABORATORIO DI INFORMATICA, IL TEAM DIGITALE**

Il ruolo dei suddetti soggetti consiste in :

- Stimolare la formazione interna negli ambiti di sviluppo della scuola digitale e fornire consulenza e informazioni al personale in relazione ai rischi on line ed 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
- Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti
- Coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la scuola digitale

3. **REFERENTE BULLISMO**

Per l'attuazione delle finalità di cui all'articolo 1, comma 1, del disegno di legge del Senato n. 1261 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" la scuola nomina un docente Referente in merito alle problematiche del bullismo e cyberbullismo.

Il ruolo del referente prevede:

- prendere parte ai corsi di formazione previsti dalla suddetta legge ai fini di garantire l'acquisizione di idonee competenze teoriche e pratiche
- organizzare attività formative per i docenti
- promuovere la conoscenza del fenomeno e gli strumenti di prevenzione dello stesso affinché le famiglie possano riconoscerlo ed intervenire in modo corretto,
- sostenere la famiglia e i minori vittime del cyberbullismo
- promuovere, in collaborazione con tutti gli insegnanti, l'educazione all'uso consapevole della rete di bambini e ragazzi, favorendo specifici percorsi didattici finalizzati a responsabilizzare gli stessi minori e a promuoverne la consapevolezza in ordine ai rischi, oltre che alle opportunità

- garantire, a questo riguardo, la continuità curricolare tra i diversi ordini di scuola e in modo particolare tra la secondaria di primo grado e la secondaria di secondo grado, secondo quanto previsto dal decreto.

4. DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

Il ruolo del DSGA 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 all'interno della scuola e fra la scuola e le famiglie

5. 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
- controllare l'uso delle tecnologie digitali da parte degli alunni durante le lezioni e in ogni altra attività scolastica
- 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 bisogni , difficoltà o disagi espressi degli alunni rilevati a scuola e connessi con l'utilizzo delle TIC al fine di approfondire e concordare coerenti linee di interventi educativi

- segnalare qualsiasi problema o proposta di carattere tecnico organizzativo ovvero esigenza di carattere informativo all'AD 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 di rischi nell'uso delle TIC

- segnalare al DS e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tic o di internet per l'adozione delle procedure previste nelle norme

6. ALLIEVI

Il ruolo degli allievi 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, difficoltà o richieste di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori

7. GENITORI

Il ruolo dei genitori degli alunni include i seguenti compiti :

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC 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

SEZIONE 2

Condivisione e comunicazione della Policy all'intera comunità scolastica

a) Condividere e comunicare la politica 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 saranno programmati nell'ambito della disciplina TECNOLOGIA per aumentare la consapevolezza e l'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 alla 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 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 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'AD che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici
- l'AD metterà in evidenza on line strumenti che il personale potrà usare con i bambini in classe .
- 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**

- 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'Ad e i docenti della classe forniranno ai genitori indirizzi sul web relativi a risorse per lo studio e a siti idonei ed educativi per gli alunni , sistemi di filtraggio e attività educative per il tempo libero
- i genitori esperti potranno collaborare nelle attività di informazione / formazione

SEZIONE 3

GESTIONE DELLE INFRAZIONI ALLA POLICY

1) **disciplina degli alunni**

Le infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali , in relazione alla fascia di età considerate, sono prevedibilmente le seguenti :

- uso inappropriato della Rete
- 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 inadeguate
- la comunicazione incauta e senza permesso con sconosciuti

Gli interventi correttivi sono rapportati all'età e al livello di sviluppo del bambino

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 e sul Registro elettronico
- la convocazione dei genitori da parte degli insegnanti
- la convocazione dei genitori da parte del Ds
- l'eventuale provvedimento disciplinare deciso dal consiglio di classe o interclasse

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 degli 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 segnalazioni ai genitori , al Dirigente scolastico o 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 copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Ds 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 (fino a 14 anni) e della loro dipendenza dagli adulti , alcune considerazioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola , luogo in cui 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 piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone
- un utilizzo del pc, del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria materiali non idonei

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli , se dovessero risultare pericolosi per sé e/o dannosi per altri ,in relazione soprattutto a materiale o situazioni che abbiano ripercussione in ambito scolastico.

INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI

La Policy richiede l'aggiornamento del Regolamento di istituto con l'inserimento delle seguenti norme :

L’uso della postazione di lavoro è soggetto alle seguenti condizioni :

1. DIVIETI

   E' vietato installare materiale protetto da copyright. E' vietato l'uso della postazione di lavoro per i collegamenti a Internet a scopi commerciali o di profitto personale o di attività illegali. Ricordando che la responsabilità delle azioni compiute tramite una utenza è sempre del legittimo titolare , anche se compiute in sua assenza , la password ricevuta non deve essere comunicata a nessuno e non deve essere salvata su dispositivi di uso comune . Essa deve essere memorizzata dall'utente che non deve trascriverla in nessun luogo . Ogni contatto ed operazione on line che implica assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal legale rappresentante dell'istituzione .

2. USO PERSONALE

   E' consentito l'utilizzo della postazione di lavoro , in modo saltuario , a fini personali , solo se compatibile o funzionale al ruolo professionale svolto purchè non sia causa diretta o

indiretta, di disservizi dei sistemi elaborativi e dei servizi di collegamento dell'Amministrazione ; non sia causa di oneri aggiuntivi per l'Amministrazione , non interferisca con le attività lavorative dell'utente , delle attività scolastiche o con altri obblighi dello stesso verso l'Amministrazione .

3. USO DIDATTICO

- Ogni allievo è direttamente responsabile della postazione assegnatagli per le ore in cui vi svolge lezione . Agli utenti è fatto assoluto divieto di cancellare ,modificare in qualsiasi modo i files presenti sulla macchina o alterare il sistema operativo o la configurazione dei programmi e dell'hardware della macchina .
- E' fatto obbligo di adottare comportamenti idonei a non provocare danni o pericoli agli strumenti ed alle attrezzature messi a disposizione . In caso contrario l'utente dovrà porvi rimedio riparando o ripagando il danno e/o provvedendo alla pulizia o al riordino.
- Gli utenti sono tenuti a non prelevare o depositare informazioni, applicazioni o documenti che possano in qualsiasi modo arrecare danno a persone , cose o istituzioni
- E' vietato inserire file sul server o scaricare da internet software non autorizzati o materiale soggetto a copyright o a diritti di proprietà intellettuale
- Il riscontro di qualsiasi anomalia deve essere tempestivamente segnalato dagli alunni al docente e dal docente al responsabile del laboratorio
- per utilizzare CD _ROM , DVD , penne USB o altri supporti di memorizzazione personali è necessario chiedere il permesso e sottoporli al controllo anti virus
- L'utilizzo di videogames è vietato , a meno che non vi sia una finalità didattica del gioco , espressamente prevista dal docente
- Si devono rispettare le regole di decenza e morali, evitare atti e comportamenti che possano recare offesa a cose , persone o istituzioni presenti o meno sulla rete.
- E' fatto assoluto divieto di navigare in siti dai contenuti pornografici o contenenti scene di violenza , razzismo o sfruttamento dei minori
- Si deve mantenere segreto il nome, l'indirizzo, il telefono di casa, il telefono cellulare , il nome e l'indirizzo della scuola frequentata
- non si devono inviare a nessuno fotografie proprie o di amici

I docenti che accompagnano gli allievi in laboratorio o fanno usare i dispositivi di classe o i loro dispositivi (vedasi BYOD) sono tenuti a controllare che vengano rispettati i divieti sopraelencati e che l'utilizzo delle risorse tecnologiche sia finalizzato agli intenti didattici previsti .

SEZIONE 4

GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

A. **ACCESSO A INTERNET : FILTRI , ANTIVIRUS SULLA NAVIGAZIONE**

L'accesso a Internet è possibile e consentito per la didattica nel laboratorio multimediale e in classe nel caso di utilizzo delle LIM , dei pc di classe e dei dispositivi personali da parte dei docenti e degli alunni secondo quanto indicato nel regolamento BYOD in vigore nel nostro Istituto .

L'accesso dai pc dell'istituto (laboratorio e pc classi) è schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list , secondo le impostazioni date del team digitale che provvede periodicamente alla manutenzione e aggiornamento del sistema informatico del laboratorio, ove necessario richiedendo l'intervento di tecnici esterni .

Per quanto riguarda i dispositivi degli alunni, portati da casa , si rimanda al Regolamento BYOD; riguardo alla navigazione sicura con i dispositivi personali si specifica che i filtri dei dispositivi personali devono essere installati a cura dei genitori tutori dell'alunno su ciascun dispositivo

GESTIONE ACCESSI

L'accesso al sistema informatico per la didattica è consentito al personale attraverso l'assegnazione di una password . La password è comune e permette di accedere al server . Le postazioni del laboratorio e nelle classi funzionano come stazioni di lavoro e non come archivio

1. **E MAIL**

L'account di posta elettronica è solo quello istituzionale utilizzato dagli uffici amministrativi , sia per la posta in ingresso che in uscita.

2. **SITO DELLA SCUOLA**

La scuola attualmente ha un sito web . Tutti i contenuti del settore didattico sono pubblicati sotto la supervisione del docente REFERENTE DEL SITO , che ne valuta con il Dirigente Scolastico la sicurezza e l'adeguatezza sotto il profilo dell'accessibilità , della pertinenza dei contenuti , del rispetto della privacy

3. **SOCIAL NET WORK**

Attualmente nella didattica non si utilizzano social network . L'Istituzione scolastica ha però creato, col profilo della posta istituzionale del primo collaboratore, una pagina you tube per la

pubblicazione di video di attività didattiche particolarmente significative , anche per diffonderle attraverso questo canale , sul sito dell'Istituto .

Nel caso di video in cui siano ripresi gli alunni durante le attività didattiche , eventi o manifestazioni verrà acquisita specifica autorizzazione scritta dei genitori di ciascun alunno coinvolto .

4. PROTEZIONE DEI DATI PERSONALI

Il personale scolastico è " incaricato del trattamento" dei dati personali nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza. Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali AL MOMENTO DELLA STIPULA DEL CONTRATTO DI LAVORO ai fini della protezione e sicurezza degli stessi .

B. STRUMENTAZIONE PERSONALE

- PER GLI STUDENTI : gestione degli strumenti personali – cellulari tablet si rimanda al regolamento BYOD
- PER I DOCENTI : gestione degli strumenti personali

  Durante le ore di lezione non è consentito l'utilizzo del cellulare , mentre è consentito l'uso di altri dispositivi elettronici personali a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario è consentito l'utilizzo del cellulare per comunicazioni 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

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

SEZIONE 5

Secondo il disegno di legge del Senato n. 1261 Art. 1. Comma 2 , per cyberbullismo, si intende: "qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione e si intende altresì qualunque forma di furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica".

L' Istituto opererà in merito al suddetto articolo nel modo seguente:

PREVENZIONE , RILEVAZIONE E GESTIONE DEI CASI

A. PREVENZIONE

1. **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 o dello smartphone , dei pc e dei tablet della scuola collegati alla rete

Il telefono cellulare non è richiesto dalla scuola perchè non è ritenuto necessario in ambito scolastico , ma viene spesso fornito dai genitori per mantenere i contatti con i figli anche fuori dal contesto scolastico .

2. **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 tecnologie può favorire
- fornire ai genitori informativa e richiesta di utilizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (liberatoria per la pubblicazione delle foto, immagini , testi e disegni ….)
- non consentire l'utilizzo del cellulare a scuola in quanto per comunicazioni urgenti 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 solo in casi particolari ed eccezionali , ad es quando ci trova fuori dal contesto scolastico durante una visita guidata , e comunque sempre con la supervisione dell'insegnante .
- Utilizzare filtri, software che impediscono il collegamento a siti web per adulti

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 ed 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 o suggerirgli di bloccare particolari mittenti, di rimuoverli dalla lista degli amici, 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, di scaricare un'applicazione che blocchi chiamate o messaggi da numeri indesiderati o, se necessario , cambiare il numero di cellulare

- 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 agli altri, e conservare una copia di detto materiale per ulteriori indagini

- contattare la polizia postale se si ritiene che il materiale offensivo sia illegale . In caso di foto e video pedopornografici, confiscare il telefono o altri dispositivi ed evitare di eseguire download , produrne copie , condividerne link o postarne il contenuto , poiché ciò è reato per chiunque.

B . RILEVAZIONE

1. **CHE COSA SEGNALARE**

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri o riferire spontaneamente o su richiesta l'accaduto ai docenti . I fatti riferiti possono essere accaduti anche al di fuori della scuola . Anche confrontandosi periodicamente 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 il telefono cellulare si rivolge al genitore .

I contenuti pericolosi comunicati/ricevuti da altri , messi/scaricati in rete ovvero le tracce che possono comprovare l'utilizzo incauto possono essere i seguenti :

- contenuti afferenti alla privacy
- contenuti afferenti all'aggressività
- contenuti afferenti alla sessualità

2. **COME SEGNALARE : QUALI STRUMENTI E A CHI**

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi sul suo telefono ogni messaggio/voce/testo/immagine , conservando così il numero del mittente.

Gli insegnanti anche con l'ausilio tecnico dell'AD provvedono a conservare le prove della condotta scorretta o dell'abuso rilevate sui pc della scuola : la data e l'ora , il contenuto dei messaggi , e , se possibile , l'ID del mittente o l'indirizzo web del profilo e il suo contenuto.

Qualora ci si dovesse accorgere che l'alunno , usando il computer , si sta servendo di un servizio di messaggeria istantanea , l'insegnante può copiare e incollare e stampare la conversazione . Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting site e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word.

Per le 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 DS e per le condotte criminose alla Polizia .

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno , le notizie raccolte sono comunque comunicate ai genitori e al ds ; 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 rilevanti si applica il Regolamento di istituto per INFRAZIONI GRAVI

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 competenti.

Ai fini della denuncia , la relazione deve essere fatta nel modo più dettagliato possibile indicando : il fatto , il giorno dell'acquisizione del fatto , nonché le fonti di prova , 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.

3. **GESTIONE DEI CASI**

DEFINIZIONE DELLE AZIONI DA INTRAPRENDERE A SECONDA DEI CASI

1. **Gestione dei casi di immaturità**

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo da attrarre l'attenzione, che richiedono una procedura di registrazione.

Curiosità , manifestazioni di interesse tra pari , idee e fantasie sulla sessualità sono espressioni del progressivo sviluppo dell'alunno e dei molteplici messaggi che gli giungono quotidianamente attraverso i media , i discorsi degli altri bambini e degli adulti .

I comportamenti cosiddetti " quasi aggressivi", che spesso si verificano fra coetanei, la presa in giro " per gioco" , effettuata anche in rete, mettono alla prova la relazione coi compagni, la supremazia o la parità tra i soggetti , e l'alternanza e la sperimentazione dei diversi ruoli .

Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dagli adulti e pertanto luogo di complicità e di piccole trasgressioni , di scambi confidenziali condivisa fra gli amici nella rete o con il cellulare.

Detti comportamenti sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza , di rispetto per gli altri per evitare che possano degenerare , diventare pericolosi per sé o offensivi e minacciosi per gli altri .

2. **Gestione dei casi i prepotenza o prevaricazione**

I comportamenti definibili di BULLISMO possono esprimersi nelle forme più varie e non sono tratteggiabili a priori , se non contestualizzandoli.

Le caratteristiche che aiutano ad individuarli ed a distinguerli dallo scherzo 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 non da un solo soggetto , ma in genere da un gruppo.

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

- invio di sms, messaggi in chat , mail offensive o di minaccia
- diffusione di messaggi offensivi ai danni della vittima , attraverso la divulgazione di sms o e-mail nelle mailing list o nelle chat line
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata

Il bullismo può originarsi anche dall'esasperazione di conflitti presenti nel contesto scolastico .

Il conflitto , presente in ogni normale interazione, 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.

Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire , ma affrontano e intervengono sul gruppo classe coinvolgendo anche i genitori .

- l'elemento fondamentale è la corretta ricostruzione dell'ambiente sociale in cui tale fenomeno si verifica

- Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team docente con le famiglie

Vengono intrapresi anche percorsi di sostegno alle vittime volti a incrementarne l'autostima , mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali .

In relazione alle manifestazioni socio affettive fra pari i docenti intervengono per favorire nei ragazzi un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di confidenza ed imparare ad apporvisi , per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche " a distanza" sgradevoli e strani , per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire che l'interazione on line deve sottostare a delle regole di buon comportamento, né più né meno di quelle della vita reale.

Qualora la scuola rilevi una situazione psico-socio-educativa particolarmente problematica , convoca i genitori per valutare con loro a quali risorse territoriali possono rivolgersi.

3. **Gestione degli abusi sessuali**

Le forme di abuso sono diventate ancora più subdole in seguito alle possibilità offerte dai nuovi mezzi di comunicazione e il loro utilizzo non fa che acuire il problema .

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 o a richieste di fotografie o video . Spesso l'adulto si finge minorenne.

La denuncia all'Autorità giudiziaria o agli organi di polizia da parte degli insegnanti o del Ds , costituisce il passo necessario per avviare un intervento di tutela della vittima e un procedimento penale nei confronti del presunto colpevole.

Il compito della scuola dunque non è solo quello di segnalare e denunciare , ma anche quello di educare alla prevenzione .

SEZIONE 6

MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto ogni anno , con l'alternarsi delle classi quinta e seconda secondaria.

Tale monitoraggio sarà curato dal Ds con la collaborazione dell'AD ed ai docenti delle classi , tramite questionari e conversazione. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle TIC e di internet . Il monitoraggio sarà rivolto anche agli insegnanti , al fine di valutare l'impatto della policy e le

necessità di eventuali miglioramenti . L'aggiornamento della policy sarà curato dal ds , dall'AD , dagli organi Collegiali , a seconda degli aspetti considerati

SEZIONE 7

FORMAZIONE

- **FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA**

Il corpo docente ha partecipato estesamente a corsi di formazione sia nell'ambito di piani nazionali che su iniziative organizzate dall'istituzione o dalle scuola associate in Rete e possiede generalmente una buona 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 . Il percorso complesso della formazione specifica dei docenti per l'utilizzo delle TIC nella didattica prosegue grazie a momenti di aggiornamento (corsi PON e Rete) e autoaggiornamento personale o all'interno dell'Istituto e on line .

Sono disponibili per i docenti varie risorse :

- programma il futuro
- CATALOGO FORMATIVO DEL PNFD

- **FORMAZIONE DEI DOCENTI SULL'UTILIZZO 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 e a cui accedono sempre di più ed autonomamente anche i ragazzi

Tramite il sito è possibile l'accesso diretto a

progetto GENERAZIONI CONNESSE : MATERIALI informativi sulla sicurezza in Internet per l'approfondimento personale , per le attività con gli studenti e gli incontri con i genitori costituiti da video , guide , manuali , link e contributi della Polizia di Stato, dell'Arma dei carabinieri e di Telefono Azzurro

- **SENSIBILIZZAZIONE DELLE FAMIGLIE**

L'Istituto ha attivato iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete , promuovendo la conoscenza delle numerose situazioni di rischi on line . A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate , messo a disposizione dei 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 o smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo .

Sul sito scolastico sulla bacheca relativa a GENERAZIONI CONNESSE sono già stati messi in condivisione materiali dedicati ad alunni e famiglie che possono servire come spunti di approfondimento e confronto .

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

REGOLAMENTO AULA INFORMATICA

PLESSO FAVRIA G. VIDARI – FRONT DON MILANI –

BUSANO PRIMARIA

Il Laboratorio di Informatica in assenza di utenti , deve sempre essere rigorosamente chiuso a chiave e quindi non accessibile .

Per accedervi è necessario che l'insegnante interessato richieda la chiave al personale in servizio al piano il quale provvederà anche a far firmare l 'apposito registro , che dovrà poi essere controfirmato al momento della riconsegna della chiave .

MODALITA' DI ACCESSO

L'accesso al laboratorio di informatica è permesso solamente agli studenti accompagnati dal loro insegnante .

I docenti della classe sono tenuti , come sopra indicato , ad apporre la loro firma sull'apposito registro ogni volta che utilizzano il laboratorio e a svolgere azione di controllo affinchè non si verifichino manomissioni da parte degli studenti .

In Laboratorio è vietato consumare cibi e bevande

I locali e le attrezzature devono essere mantenuti in situazione di ordine e pulizia

MODALITA' DI USO

Ogni utente è tenuto al corretto uso dei locali e della dotazione hardware e software.

Ogni utente deve essere a conoscenza della legislazione vigente ed in particolare del Regolamento e-safety di Istituto , pertanto è responsabile delle proprie azioni .

Gli utenti non possono installare programmi o pacchetti software se non autorizzati dal responsabile del Laboratorio .

Non si possono modificare programmi o pacchetti software già installati sui computer, né eliminare file che non siano di esclusivo uso personale .

Gli studenti sono tenuti a mantenere la loro postazione nel corso della lezione e non devono modificare l'assetto dei pc.

E' opportuno che al termine di ogni lezione l'insegnante controlli che i computer si trovino nell'assetto standard anche per individuare eventuali responsabilità di manomissione o altre problematiche .

Si ricorda che i vari pc sono postazioni di lavoro e non di archivio , pertanto i file creati andranno rimossi dai pc e salvati su chiavette USB personali o di classe .

Nel caso di individuazione di virus o di altre anomalie , l'insegnante avrà cura di segnalare immediatamente il fatto all'Animatore Digitale .

STAMPA

Si raccomanda di ridurre al minimo le stampe e si ricorda che la realizzazione di attività che richiedano un cospicuo consumo di inchiostro deve essere concordata col Responsabile di laboratorio

ACCESSO A INTERNET

Per l'accesso a internet si rimanda al Regolamento e-safety policy dell'istituto SEZIONE 3 , sia come indicazioni che come DISCIPLINA DELLE INFRAZIONI .

APPROVATO DAL COLLEGIO DEI DOCENTI IN DATA 18 MAGGIO 2017

APPROVATO AGGIORNAMENTO DAL COLLEGIO DEI DOCENTI DEL 25 OTTOBRE 2018

APPROVATO DAL CONSIGLIO DI ISTITUTO DEL 12 NOVEMBRE 2018