



Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO STATALE "A. MANZONI"

Piazzale Martiri Vimercalesi, 1 - 20871 Vimercate (MB) Tel 039668505 – 039.6918710 Fax 039.666945
e-mail: miic8ew00b@istruzione.gov.it pec: miic8ew00b@pec.istruzione.gov.it
Codice Meccanografico **MIIC8EW00B** - Codice Fiscale **94054710150**
Sito: www.icmanzonivimercate.it

**IL PRESENTE DOCUMENTO E' STATO PREDISPOSTO DA UN GRUPPO DI
DOCENTI E CONDIVISO CON IL DIRIGENTE SCOLASTICO.
E' stato deliberato
dal COLLEGIO DEI DOCENTI il 17 maggio 2018 e
dal CONSIGLIO DI ISTITUTO il 6 novembre 2019.**

E-Safety Policy

INDICE

1. Introduzione

- 1.1 Fondamento e Scopo della Policy
- 1.2 A chi è rivolta?
- 1.3 Ruoli e Responsabilità
- 1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica
- 1.5 Gestione delle infrazioni alla Policy
- 1.6 Monitoraggio dell'implementazione della Policy e suo aggiornamento
- 1.7 Integrazione della Policy con Regolamenti esistenti

2. Formazione e Curricolo

- 2.1 Educazione alla sicurezza online e all'uso delle TIC
- 2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica
- 2.3 Sensibilizzazione/educazione delle famiglie

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

- 3.1 Accesso ad internet, filtri, antivirus
- 3.2 Sito web della scuola
- 3.3 Cloud computing: il registro elettronico, la segreteria digitale
- 3.4 Social network
- 3.5 Protezione dei dati personali

4. Strumentazione personale: uso di cellulari e dispositivi mobile (notebook, laptop, tablet)

Premessa

- 4.1 Norme generali sull'uso device mobili personali a scuola
- 4.2 Indicazioni generali per acquisizione di immagini e video digitali
- 4.3 Per gli studenti: gestione degli strumenti personali
- 4.4 Per i docenti, educatori, esperti di progetto: gestione degli strumenti personali
- 4.5 Per personale della scuola: gestione degli strumenti personali

5. Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

5.2 Rilevazione

APPARATI (da considerarsi parte integrante di questo documento e messi in allegato separato)

1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative/pratiche ad esempio per la rilevazione, il monitoraggio e la gestione delle segnalazioni e gestione dei casi.

1. Introduzione

Per "Policy" si intende l'insieme dei principi, linee guida, decisioni, provvedimenti che un'organizzazione pone in essere per perseguire specifici obiettivi ed indicare il modo più adatto per affrontare problematiche di varia natura presenti nell'organizzazione stessa.

La "Policy" che qui viene presentata riguarda tutte le persone che, direttamente o indirettamente, sono coinvolte nell'ICS "A. Manzoni".

Essa non ha valenza statica ma sarà continuamente monitorata negli esiti e adattata ai cambiamenti che avvengono nel tempo.

La Policy è un documento programmatico che impegnerà la scuola e i suoi attori anche per gli anni futuri: di conseguenza quanto si troverà di scritto sarà realizzato gradualmente nel tempo, monitorato negli esiti rispetto alle attese prefissate, ampliato e modificato a seconda delle condizioni che man mano si manifesteranno o ci verranno suggerite dalle agenzie di riferimento.

1.1 Scopo della Policy

Sia a livello internazionale che nel contesto italiano la presenza sempre più diffusa, anche tra i più giovani, delle tecnologie digitali nella vita di tutti i giorni apre nuove opportunità ma necessita di regolamentazione in vista di un loro uso sicuro, consapevole e positivo.

Lo scopo dell' E-Safety Policy è di stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie: salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto; assistere il personale della scuola e lavorare in modo sicuro e responsabile con le tecnologie della comunicazione; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico; impostare misure per la prevenzione, per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole/non adeguato delle tecnologie digitali; garantire che tutti i membri della comunità scolastica siano consapevoli che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari.

Le principali aree di rischio per la nostra comunità possono essere riassunte come segue:

Contenuto:

- L'esposizione a contenuti dannosi e non appropriati
- Siti web che promuovono stili di vita e comportamenti dannosi

- Contenuti che spingono all'odio
- Validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online

Contatto:

- Grooming (adescamento online)
- Cyberbullismo in tutte le forme
- Il furto di identità, comprese le password

Condotta:

- Violazione della privacy, tra cui la divulgazione di informazioni personali o di dati (foto, video, voce) senza autorizzazione dei soggetti interessati
- Reputazione digitale
- Salute e benessere: dipendenza da Internet e quantità di tempo speso online
- Sexting
- Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore)

1.2 A chi è rivolta?

Questa Policy si applica a tutta la comunità dell'ICS "A. Manzoni di Vimercate":

- ai bambini, che frequentano la scuola dell'Infanzia e la scuola Primaria;
- ai ragazzi della Secondaria di primo grado;
- a tutti i docenti che svolgono la loro attività di insegnamento nella nostra scuola, anche per brevi periodi;
- al Dirigente Scolastico e al Direttore dei Servizi Generali e Amministrativi;
- a tutto il personale amministrativo e a tutti i collaboratori scolastici
- a tutti gli operatori/professionisti e/o volontari che entrano a scuola - in particolare a quelli che si mettono in relazione con i nostri ragazzi (a titolo di esempio: educatori, esperti di progetto, assistenti di mensa)
- ai tutti i genitori

1.3 Ruoli e Responsabilità

Ruolo	Responsabilità
Dirigente Scolastico	<ul style="list-style-type: none"> • Fornire sistemi per un uso sicuro delle TIC, Internet. • Garantire che l'Istituto segua le pratiche migliori possibili nella gestione dei dati e nella sicurezza delle informazioni. • Garantire a tutto il personale una formazione adeguata sulla sicurezza online. • Essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy.
Animatore digitale, team e referente Cyber Bullismo; tecnici aule informatiche	<ul style="list-style-type: none"> • Promuovere la cultura della sicurezza online. • Assicurare che l'educazione alla sicurezza online sia incorporata nel Curricolo di Competenze Digitali. • Garantire che tutto il personale sia a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy. • Facilitare la formazione e la consulenza per tutto il

	<p>personale.</p> <ul style="list-style-type: none"> • Collaborare, al bisogno e se è il caso, con il personale tecnico (anche esterno) in forza alla scuola.
Referente Cyber Bullismo	<ul style="list-style-type: none"> • Tenere aggiornato un registro degli incidenti di sicurezza online. • Supervisionare qualsiasi sondaggio e feedback in materia di sicurezza online. • Ricevere comunicazione/monitorare situazioni di rischio o conclamate. • Riferire tempestivamente al Dirigente per prendere contatti con le Autorità Locali e agenzie competenti.
Gli insegnanti	<ul style="list-style-type: none"> • Leggere, comprendere e approvare la E-Safety Policy. • Educare alla sicurezza online nello svolgersi del curriculum della propria disciplina. • Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online. • Garantire che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano pienamente consapevoli dei problemi relativi ai contenuti elettronici (come ad esempio le leggi sul copyright).
Tutto il personale dell'Istituto; esperti esterni, educatori, volontari	<ul style="list-style-type: none"> • Leggere, comprendere, aderire alla E-Safety Policy e aggiornarsi sulle relative modifiche. • Segnalare qualsiasi abuso sospetto o qualsiasi problema al Dirigente o al referente del Cyberbullismo. • Avere la consapevolezza delle problematiche di sicurezza online prese in esame dalla scuola con questo documento. • Assumere comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie.
Gli studenti (dal terzo anno della Scuola Primaria)	<ul style="list-style-type: none"> • Leggere, comprendere e accettare la E-Safety Policy. • Avere una buona comprensione delle capacità di ricerca, della necessità di evitare il plagio e di rispettare normative sul diritto d'autore. • Capire l'importanza di segnalare l'abuso, l'uso improprio o l'accesso a materiali inappropriati. • Sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando utilizza la tecnologia online. • Capire l'importanza di adottare sempre comportamenti sicuri e buone pratiche di sicurezza online quando usano le tecnologie digitali. • Essere consapevoli che la E-Safety Policy di sicurezza online della scuola può aiutarli anche fuori dalle mura e/o dall'orario scolastico. • Conoscere la politica relativa all'utilizzo dei telefoni cellulari, fotocamere digitali e dispositivi portatili.

	<ul style="list-style-type: none"> • Assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.
I genitori	<ul style="list-style-type: none"> • Leggere, comprendere e controfirmare la E-Safety Policy . • Sostenere la scuola nel promuovere la sicurezza online. • Accedere al sito web della scuola e al registro elettronico in conformità a quanto prescritto. • Confrontarsi con la scuola in caso di preoccupazioni circa l'uso della tecnologia online o offline da parte dei loro figli. • Approvare un accordo sull'uso accettabile delle tecnologie che può comprendere l'uso da parte della scuola di immagini fotografiche e video ai fini di promulgazione/documentazione didattica e partecipazione a progetti/concorsi promossi da Enti di affermata reputazione in ambito educativo o territoriale.

Al fine di garantire una gestione il più possibile corretta, la scuola si attrezza per evitare comportamenti che non rientrano nelle norme che il Collegio dei Docenti ha definito in proposito, come:

- alterare i parametri di protezione dei computer in uso
- utilizzare la rete per interessi privati e personali che esulano dalla didattica
- non rispettare le leggi sui diritti d'autore
- navigare su siti non accettati dalla protezione interna della scuola

La scuola inoltre mette in atto alcune strategie:

- il sistema informatico è periodicamente controllato dai responsabili e dai consulenti esterni
- verifiche antivirus sono condotte periodicamente sui computer
- vengono controllati periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina
- è fatto divieto di installare e scaricare da Internet software non autorizzati
- l'utilizzo di CD, chiavi USB e altre memorie esterne devono essere autorizzati dai docenti e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete
- il Dirigente Scolastico si riserva di limitare l'accesso e l'uso della rete Internet secondo normali canali di protezione presenti nei sistemi operativi.

1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica

La Policy sarà comunicata al personale/alunni/comunità e persone che fruiscono del nostro servizio di istruzione/educazione nei seguenti modi:

- sul sito della scuola una volta approvata in modo definitivo
- via mail agli stakeholders che lo richiedano

Per tutto il personale sono previsti regolari aggiornamenti e nuova formazione in materia di sicurezza online.

1.5 Gestione delle infrazioni alla Policy

L'Istituto prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando su un computer della scuola. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.

Il Referente per il Cyberbullismo è la prima persona da contattare per qualsiasi incidente. Qualsiasi sospetto, rischio, violazione va segnalato in giornata al Referente per il Cyberbullismo che riferisce al Dirigente.

Qualsiasi allerta di uso improprio del personale va sempre riferita direttamente al Dirigente Scolastico, a meno che esso si riferisca al Dirigente Scolastico stesso; in questo caso si riferisce direttamente alle autorità di competenza. Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni.

Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.

1.6 Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy sarà riesaminata annualmente e/o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola.

Sarà rivista in relazione a norme di maggior valore come regolamenti o Policy emanati dal MIUR o eventuali leggi dello Stato.

1.7 Integrazione della Policy con Regolamenti esistenti

La E-Safety Policy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto, in particolare con il ***Regolamento di disciplina*** con relativa tabella di sanzioni previste. Tutto ciò che qui non è normato è da considerarsi regolamentato secondo tale disciplina generale.

2. Formazione e Curricolo

2.1 Educazione alla sicurezza online e all'uso delle TIC

L'Istituto si propone di definire un chiaro e progressivo programma di educazione alla sicurezza online e uso delle TIC, all'interno del curricolo delle competenze digitali e di cittadinanza digitale.

Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e alle loro esperienze, quali:

- sviluppare strategie per valutare e verificare le informazioni prima di accettarne l'esattezza,
- sapere come restringere o affinare una ricerca,
- capire quali sono i comportamenti sicuri e responsabili nell'utilizzare Internet,
- capire come le fotografie possono essere manipolate,
- capire perché "amici" online potrebbero non essere chi dicono di essere e comprendere perché fare attenzione in un ambiente online,
- capire il motivo per il quale non dovrebbero inviare e condividere resoconti dettagliati delle loro vite personali e informazioni di contatto,
- capire il motivo per il quale non devono pubblicare foto o video di altri senza il loro permesso,
- comprendere l'impatto del bullismo online,
- sapere come segnalare eventuali abusi e come chiedere aiuto ai docenti, ai genitori, se si verificano problemi,
- imparare a rispettare e riconoscere i diritti di proprietà intellettuale e il diritto d'autore, essere a conoscenza di problemi intorno al plagio e saper controllare il copyright .

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

Il nostro Istituto ha avviato già dall' a.s. 2015/16 dei percorsi di formazione destinati ai docenti sull'utilizzo e l'integrazione delle TIC nella didattica e si impegna a continuare nel:

- formare i docenti su **nuove metodologie di insegnamento/apprendimento** con attenzione al saper gestire didatticamente gli strumenti hardware, software, social, cloud computing individuandone punti di debolezza/forza anche in termini di sicurezza;
- dare formazione regolare al personale della scuola in materia di sicurezza online e a renderlo partecipe del il programma di educazione alla E-Safety.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Valuta inoltre l'adesione a progetti appositi di formazione presentati da enti e associazioni, come già avvenuto in passato.

2.3 Sensibilizzazione/formazione delle famiglie

Questo Istituto, in collaborazione con il Comitato genitori, si impegna a informare i genitori sulle problematiche legate alla sicurezza online e all'uso delle TIC.

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

3.1 Accesso ad Internet, filtri, antivirus, password

L' Istituto gestisce linee Internet dedicate esclusivamente alla didattica (in tutte le sedi) e una linea esclusiva per la parte amministrativa. Ogni sede dispone di aule informatiche; quasi tutte le classi (nella primaria e secondaria) sono dotate di computer portatili collegati alla LIM che accedono ad Internet attraverso rete WIFI. Nel laboratorio informatico sono presenti pc portatili e fissi. I primi accedono tramite rete WIFI, i secondi attraverso rete LAN; su tutti è installato un programma antivirus.

Gli studenti non possono accedere con i loro dispositivi alla rete Internet della scuola. I docenti possono accedere con i loro dispositivi personali alla rete dopo autorizzazione dei docenti tecnici informatici. Ciascun insegnante dispone di una password personale per il registro elettronico che non può essere comunicata a terzi, né agli alunni.

I computer portatili presenti nelle aule non richiedono una password di accesso per l'accensione e l'utilizzo dei programmi base; esiste una password amministratore per apportare modifiche ai computer e installare programmi.

Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante.

3.2 Sito web della scuola

Il sito web dell'Istituto è gestito dal docente **Animatore Digitale e dagli impiegati di Segreteria**. L'amministratore del sito è la società 3s srl Solution Services Systems. L'accesso a tale area è nominativo.

La maggior parte del materiale è prodotto direttamente dell'Istituto, che detiene il diritto d'autore sui documenti pubblicati sul sito.

Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. L'Istituto cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.

Quando viene pubblicato o linkato il lavoro di altri, si mettono gli accrediti alle fonti utilizzate e si indicano chiaramente l'identità o lo stato dell'autore.

3.3 Cloud computing: il registro elettronico, la segreteria digitale

Il sito istituzionale viene integrato da altri due ambienti, i cui dati sono di proprietà dell'Istituto ma sono mantenuti e ne viene garantita la sicurezza da terzi: il registro digitale (Gruppo Spaggiari Parma) e la segreteria digitale (Gruppo Spaggiari Parma).

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico è spiegato alle famiglie nel corso del primo consiglio di classe dell'anno scolastico e la pubblicazione delle informazioni attraverso tale strumento

assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a.

Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del team/consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

Il caricamento di informazioni su registro elettronico/segreteria digitale è condiviso tra i diversi membri del personale in base alle loro competenze: ad esempio tutti gli insegnanti di classe possono caricare informazioni nelle loro aree di pertinenza.

3.4 Social network

Personale, collaboratori, esperti, educatori

- Il personale è istruito e obbligato a mantenere sempre la comunicazione professionale separata da quella personale/privata.
- Gli insegnanti, esperti ed educatori sono formati a *non organizzare a titolo personale spazi su social network* da usare con gli studenti: questi devono essere autorizzati dalla dirigenza e devono riguardare progetti didattici di divulgazione e la documentazione dei processi di apprendimento.
- Gli insegnanti, esperti ed educatori sono formati a *non aprire i loro spazi ai loro studenti*: si devono usare i sistemi dedicati e istituzionali della scuola per tali comunicazioni.

Il personale della scuola in uso privato di spazi social:

- non fa riferimento a studenti/alunni, genitori/tutori o personale scolastico;
- **non** dovrebbe essere **amico online** di qualsiasi alunno/studente;
- non entra in discussioni online su questioni personali relative agli stessi membri della comunità scolastica;
- non attribuisce opinioni personali alla scuola o alla sua dirigenza o alle autorità locali;
- non deve compromettere il ruolo professionale e non deve portare discredito all'Istituto con le sue opinioni personali.

Gli studenti

- Agli studenti vengono insegnati i **comportamenti accettabili e di sicurezza** da assumere sui social networking: come segnalare abusi, intimidazioni o vessazioni, atti di bullismo attraverso un apposito percorso di educazione all'uso sicuro dei social network.
- Gli studenti sono tenuti a firmare e seguire la nostra Policy adattata alla propria età.

Genitori:

- I genitori vengono istruiti sui rischi di utilizzo dei social networking e i nostri protocolli attraverso la Policy.

3.5 Protezione dei dati personali:

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di E-Safety.

Il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori. Un telefono o una e-mail della scuola sarà fornito al personale cui è richiesto il contatto con la componente studentesca o con i genitori.

Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati, a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli. All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire **l'uso didattico di immagini e video** delle/dei minori secondo i principi sopra indicati.

Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

4. Strumentazione personale: uso dei cellulari e dispositivi mobile (notebook, laptop, tablet)

La possibilità di portare a scuola propri device (BYOD, Bring Your Own Device) è da considerarsi un'opportunità didattica e professionale.

Questa opportunità ci porta a considerare che il loro uso a scuola da parte dei bambini e dei ragazzi è concordato con i genitori dagli insegnanti che useranno tali strumenti in classe solo in **funzione didattica. Ogni altro uso è vietato.**

4.1 Norme generali sull' uso di device mobili personali a scuola

Il personale, esperti di progetto, gli studenti e i genitori o i visitatori che portano nell'Istituto i device di loro proprietà sono **responsabili** del proprio dispositivo e lo portano nell'Istituto a proprio rischio.

Se il device si rompe, viene smarrito o danneggiato, vengono persi dei dati ecc.. la scuola non deve essere considerata responsabile della sicurezza di tali dispositivi/dati né deve farsi carico di eventuali risarcimenti.

L'Istituto si riserva il diritto di cercare contenuti in qualsiasi dispositivo mobile presente nei locali della scuola in cui vi è il ragionevole sospetto che potrebbe contenere materiale illegale o indesiderabile (es. la pornografia, la violenza o il bullismo, registrazioni di qualsiasi genere vietate, ecc...). L'ispezione avverrà alla presenza di un pubblico ufficiale.

4.2 Indicazioni generali per acquisizione di immagini e video digitali

In questo Istituto:

- chiediamo esplicito permesso dei genitori/tutore legale per utilizzare fotografie digitali o video che coinvolgono il loro figlio. Questa autorizzazione viene sottoscritta all'atto dell'iscrizione;
- ci impegniamo a non identificare alunni in materiali fotografici online o includere i nomi completi degli alunni nei titoli di qualsiasi cosa pubblicata e prodotta in video/DVD;
- accettando e sottoscrivendo questa Policy, ***i docenti si impegnano secondo le clausole dette nell'uso dei device personali per scattare foto/fare dei video ad alunni;***
- gli alunni impareranno come le immagini possono essere manipolate nel percorso di educazione alla sicurezza online;
- gli studenti saranno aiutati a riflettere sull'opportunità di pubblicazione di foto personali su qualsiasi spazio di rete social. Verranno informati su come mantenere attive e alte le impostazioni di privacy e personali rispetto ad un possibile pubblico;
- agli alunni viene insegnato che non devono pubblicare immagini, registrazioni audio o video di altri senza permesso. Verranno loro spiegati i rischi connessi al fornire informazioni attraverso le immagini (tra cui il nome del file), che rivelano l'identità degli altri e la loro posizione. Impareranno la necessità di mantenere i loro dati sensibili al sicuro e cosa fare se sono oggetti di stalking o abusi.

4.3 Per gli studenti: gestione degli strumenti personali

- La scuola consiglia vivamente a tutti gli studenti di **non portare** telefoni cellulari e dispositivi mobile personali a scuola.
- Per le scuole primarie si vieta ai genitori la possibilità di far portare a scuola ai loro bambini il telefono cellulare/tablet se non per attività didattiche stabilite dal docente.
- Per la scuola dell'infanzia il divieto è categorico.
- Gli studenti della scuola secondaria possono portare il telefono a scuola, ma lo devono tenere spento e riposto in luogo non visibile durante l'intera permanenza a scuola. In caso di violazione a tale regola, il cellulare in uso verrà ritirato dagli insegnanti, dopo aver richiesto allo studente lo spegnimento, sarà consegnato spento in segreteria/presidenza dove lo studente potrà ritirarlo al termine della mattinata prima di tornare a casa. In ogni caso verrà avvisata telefonicamente la famiglia (*integrazione del settembre 2019, delibera del 3.10.2019 C.d.I.*).
- Telefoni e dispositivi non devono essere mai usati durante gli esami o prove nazionali. Questo porta alla esclusione dall'esame stesso e quindi all'immediata ripetizione dell'intero anno scolastico.
- Gli studenti sono responsabili della **custodia** del loro numero telefonico che non deve essere divulgato o gli ID/password personali. I ragazzi saranno guidati ad usare in modo appropriato e sicuro i loro smartphone/personal device e saranno istruiti sui limiti e le conseguenze di comportamenti non adeguati/non accettati.

Più in particolare è possibile distinguere le due seguenti situazioni:

Caso 1

1. uso del telefono cellulare/tablet/altri dispositivi mobile personali ad **uso assimilabile al privato** per chiamate, sms, messaggistica in genere, gioco, ecc.

Caso 2

2. **BYOD**: utilizzo delle funzioni, tipiche degli smartphone (foto, video, scrittura collaborativa e condivisione di documenti, varie applicazioni...), comuni anche a tablet e altri dispositivi mobili (laptop o notebook, orologi digitali), che possono avere una rilevanza e un possibile impiego nella didattica (ci si riferisce anche alle situazioni in cui i ragazzi stiano usando **strumenti mobile di proprietà dell'Istituto** per le attività didattiche a scopi professionali).

Caso 1

Uso privato per chiamate, sms, messaggistica in genere

Si ribadisce la puntuale applicazione della normativa vigente: pertanto **l'uso di mobile device non è consentito** per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica, giocare, ecc.

- Il divieto si applica all'orario delle lezioni e vale anche negli intervalli e nelle altre pause dell'attività didattica.
- L'estensione del divieto agli altri momenti di permanenza a scuola (intervallo, mensa, cambio dell'ora, ecc.), oltre a rispondere a necessità organizzative e di controllo, ha una **motivazione educativa**. Riteniamo infatti importante valorizzare momenti di relazione positiva tra gli studenti, evitando atteggiamenti di esclusione, di isolamento e di separazione dalla vita scolastica reale.

- Per quanto riguarda uscite, visite guidate e viaggi di istruzione, è fatto divieto agli alunni di utilizzare smartphone proprio o altrui (salvo eccezioni valutate dalla Dirigente Scolastica). Tale proibizione risponde a un'esigenza prettamente educativa, tesa a favorire la socializzazione e le relazioni dirette tra pari. Pertanto gli studenti sono tenuti, per l'intera durata dell'uscita, a mantenere i dispositivi spenti e riposti nello zaino e a realizzare eventuali fotografie unicamente mediante l'uso di macchine fotografiche. La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola (*integrazione del settembre 2019, delibera del 3.10.2019 C.d.I.*).
- **Le famiglie sono invitate a collaborare** strettamente con l'Istituto, nello spirito della **corresponsabilità educativa**, evitando ad esempio di inviare messaggi o effettuare chiamate ai telefoni dei propri figli, durante l'orario scolastico o visite di istruzione.
- Se portati, gli alunni sono tenuti a mantenere i loro telefoni/device spenti e riposti in luogo non visibile durante l'intera permanenza a scuola, salvo quanto previsto nel caso 2 di questo paragrafo.
- Si deve severamente evitare di essere raggiunti da qualsiasi notifica o segnalazione, eventi particolarmente distraenti e disturbanti durante l'attività didattica.

Le contravvenzioni alle prescrizioni e divieti di cui a questo caso 1 sono **sanzionate** secondo quanto previsto nei Regolamenti di Istituto vigenti.

Caso 2 BYOD

Utilizzo delle funzioni che possono avere una rilevanza e un impiego nella didattica

In questo caso l'uso **di smartphone, tablet e altri dispositivi mobili personali, è consentito.**

- Ricordiamo ai ragazzi che i device che usano **sono loro solo nominalmente** ma che, a tutti gli effetti, appartengono all'adulto che ha stipulato il contratto o li ha comprati.
- I dispositivi mobili personali verranno utilizzati unicamente durante le lezioni o il tempo scuola formale solo come parte di un'attività curriculare e secondo le modalità prescritte dall'insegnante e con **esclusiva finalità didattica**; in queste situazioni vanno comunque tenuti in **modalità silenziosa**.
- Quando gli insegnanti faranno portare il device agli alunni questo dovrà essere caricato a casa.
- Nei momenti di non utilizzo, i device devono essere tenuti spenti (non è ammessa la modalità silenzioso) e debitamente conservati fuori dalla vista fin dall'arrivo a scuola.
- Gli studenti non possono prendere in prestito dispositivi di altri studenti.
- Immagini, video, registrazioni vocali possono essere effettuate previo consenso della persona o persone in questione e con l'autorizzazione dell'insegnante.
- I ragazzi non devono caricare/postare o condividere fotografie, video, registrazione audio o qualsiasi altra informazione che riguarda sé e anche altre persone.

Tenendo conto delle recenti indicazioni del Garante della Privacy, si ribadisce che la **registrazione delle lezioni** è possibile solo per usi strettamente personali e, pertanto, previa autorizzazioni di tutte le parti coinvolte. La diffusione di tali contenuti è inoltre sempre subordinata al consenso da parte delle persone ritratte/riprese

(minori e non; se minori l'autorizzazione va richiesta ai tutori legali/genitori) e della dirigenza della scuola.

Si richiama l'attenzione degli alunni sulle **possibili conseguenze** di eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni denigratorie, intimidatorie, vessatorie. È infatti **bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità propria e di altre persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati**. Anche in questo caso si ravvisa la necessità di grande sintonia e **collaborazione tra scuola e famiglia**, in modo da favorire negli alunni lo sviluppo della necessaria consapevolezza e maturità nell'uso dei potenti strumenti ai quali hanno accesso.

In particolari casi, i consigli di classe/team o il dirigente scolastico potranno disporre specifiche condizioni d'uso, sia individuali che collettive, sempre con l'intento di ricondurre le sanzioni ad una finalità educativa e di ricercare attivamente forme di collaborazione con la famiglia.

4.4 Per i docenti, educatori, esperti di progetto: gestione degli strumenti personali

Norme generali

- Il personale **non è autorizzato a utilizzare i propri telefoni cellulari o dispositivi a titolo professionale**, come ad esempio per contattare i bambini, i ragazzi e le loro famiglie all'interno o al di fuori del proprio orario di lavoro e dall'Istituto.
- Per le visite d'istruzione potranno essere utilizzati esclusivamente nel caso si renda necessario contattare il rappresentante di classe.
- Tutti le persone che entrano nell'Istituto sono invitate a mantenere i loro telefoni e dispositivi personali sul tono silenzioso.
- I cellulari o dispositivi personali **non dovranno essere utilizzati durante l'insegnamento** a meno che non sia stato concesso un permesso dal Dirigente.
- In ogni caso si deve evitare di essere raggiunti da qualsiasi notifica o segnalazione o eventi particolarmente distraenti e disturbanti la stessa attività didattica.
- Il personale potrà utilizzare il telefono di proprietà della scuola nel caso in cui sia necessario contattare gli studenti, i genitori o altri accompagnatori.
- In caso di emergenza il docente o qualsiasi altro membro del personale della scuola (compresi educatori ed esperti di progetto), se non ha accesso immediato e semplice a un dispositivo di proprietà della scuola, è autorizzato ad utilizzare il proprio cellulare.
- Il Dirigente concede la compilazione del registro elettronico con tablet di proprietà.
- Il personale della scuola può utilizzare il proprio telefono cellulare durante i periodi di pausa, seguendo le regole generali di non disturbo delle attività.

Più in particolare è possibile distinguere le due seguenti situazioni:

Caso 1

Usò per chiamate, sms, messaggistica in genere durante le attività di docenza per uso privato

- L'uso del cellulare/tablet non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica, giocare, durante l'orario di docenza/lavoro.

- Il divieto si applica anche negli intervalli e nelle in altre situazioni che per responsabilità sono assimilabili ad **attività didattica** come mensa, cambio dell'ora, intervalli.

Caso 2

Utilizzo di funzioni che possono avere rilevanza in ambito della propria professione e un possibile impiego nella didattica nello svolgimento delle lezioni

L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità didattica e professionale.

Ribadiamo ancora che le riprese fotografiche, vocali, video potranno essere eseguite solo per **scopi didattici dichiarati**, con il **consenso** delle parti interessate (obbligatoria liberatoria dei genitori o tutori), e tenendo conto delle recenti indicazioni del Garante della Privacy.

Registrazioni o immagini effettuate durante lezioni, uscite didattiche o attività di presentazione allargate (come feste, eventi culturali ecc...) possono essere utilizzate per usi esclusivamente didattici, di divulgazione delle attività dell'Istituto e di documentazione pedagogica.

La diffusione di contenuti, da farsi solo sui canali ufficiali di proprietà della nostra scuola, è inoltre sempre subordinata all'autorizzazione del Dirigente Scolastico e, come detto, al consenso da parte delle persone ritratte/riprese.

Richiamiamo l'attenzione dei docenti, educatori, esperti sulle possibili conseguenze di eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento diversi da quelli dichiarati sopra o **che ledono la riservatezza e la dignità delle persone può far incorrere in sanzioni disciplinari e pecuniarie o in veri e propri reati.**

4.5 Per personale della scuola: gestione degli strumenti personali

Caso 1

Uso per chiamate, sms, messaggistica in genere durante le attività lavorative per uso privato

- L'uso del cellulare/tablet non è consentito per ricevere/effettuare chiamate personali, SMS o altro tipo di messaggistica, giocare, durante l'orario di lavoro.
- In ogni caso si deve evitare di essere raggiunti da qualsiasi notifica o segnalazione, eventi particolarmente distraenti e disturbanti per se stessi e gli altri durante lo svolgimento del proprio lavoro.
- Il personale è tenuto a mantenere i propri device silenziati durante lo svolgimento delle attività lavorative.

Caso 2

Utilizzo di funzioni che possono avere rilevanza in ambito della propria professione

- L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità professionale e solo in caso di **necessità particolari** da leggersi come: evacuazione dell'Istituto, emergenze.

Qualsiasi altro uso è vietato e può far incorrere in sanzioni disciplinari e pecuniarie o in veri e propri reati.

5. Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto del telefono cellulare personale o dello smartphone, dei pc della scuola collegati alla rete.

Il telefono cellulare o lo smartphone non sono generalmente 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 relativi al proprio/a figlio/a).
- **Non consentire l'utilizzo del telefono cellulare/smartphone** 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 telefono cellulare/smartphone/tablet sono **in casi particolari ed eccezionali**, ad esempio per specifiche attività didattiche concordate con il docente o quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante.

5.2 Rilevazione

Che cosa segnalare

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola.

Anche in attività didattiche ed educative di riflessione e confronto sui rischi delle comunicazioni online, 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.

Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al Referente Cyberbullismo e 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 devono essere registrate in forma scritta dal docente e comunicate ai genitori; per fatti rilevanti al Referente Cyberbullismo e 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 e in caso del Dirigente Scolastico.
- **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 "**bullismo**" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori; se non contestualizzandoli.

Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai dverbi 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, dilleggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da

un gruppo. Nel caso particolare del **Cyberbullismo** le molestie sono attuate attraverso strumenti tecnologici:

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

Il bullismo in particolare può originarsi anche dall'**esasperazione di conflitti** presenti nel contesto scolastico. Il conflitto, 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. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).

In considerazione dell'età degli alunni considerati possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, **coinvolgendo i genitori** degli allievi.

L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno. Gli **interventi mirati sul gruppo classe** sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving.

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

Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire 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 online 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 responsabilità genitoriale per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello **sportello di ascolto psicologico** attivo nell'Istituto. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ATS 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.

Annessi (da prodursi a cura della scuola) - Procedure operative per la gestione delle infrazioni alla Policy.