ISTITUTO OMINCOMPRENSIVO TRIVENTO

"NICOLA SCARANO"

# E-SAFETY POLICY

# INDICE

5. **Prevenzione, rilevazione e gestione dei casi**

- Prevenzione
- Rilevazione
- Gestione

# INTRODUZIONE

*"L'uso consapevole di Internet è fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva […] (per) la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui.*

*[...]*

*La sicurezza in Rete deve essere garantita come interesse pubblico, attraverso l'integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone."*

(DICHIARAZIONE DEI DIRITTI IN INTERNET)

## SCOPO DELLA POLICY

Il documento vuole presentare in maniera chiara ed esaustiva le linee guida dell'Istituto in materia di:

- utilizzo consapevole delle TIC nella didattica e negli ambienti scolastici
- prevenzione e gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Alla sua stesura hanno provveduto i professori referenti del progetto Generazioni Connesse per l'a.s. 2016-17, sotto la supervisione del Dirigente Scolastico. E' stato altresì fondamentale il contributo dei membri del Team per l'Innovazione Digitale, dei Coordinatori di Plesso, e il coinvolgimento di tutti i docenti e genitori che, attraverso un questionario online, hanno fornito suggerimenti e indicazioni o evidenziato eventuali problematiche presenti.

In particolare, le risposte hanno costituito il punto di partenza per :

- definire protocolli e avanzare proposte di integrazioni o modifiche al Regolamento di Istituto, riportate nel presente documento;
- delineare i bisogni formativi di docenti e genitori e raccogliere il loro punto di vista nei riguardi delle iniziative promosse dalla scuola e delle proposte avanzate;
- segnalare la necessità di strumenti didattici hardware/software e evidenziare le problematiche concernenti la sicurezza e la funzionalità dell'infrastruttura e della strumentazione ICT nei vari plessi dell'Istituto.

Nel redigere la e-policy si è tenuto conto della normativa di settore e in particolare della DICHIARAZIONE DEI DIRITTI IN INTERNET e della LEGGE A TUTELA DEI MINORI PER LA PREVENZIONE E IL CONTRASTO DEL FENOMENO DEL CYBERBULLISMO.

## RUOLI E RESPONSABILITÀ

Al fine di verificare e implementare le misure relative alla sicurezza informatica previste dal presente documento, è necessario che venga designato, all'interno dell'Istituto, un referente (o anche più di uno) che qui di seguito si indicherà con il termine **E-Policy Manager (sigla E.M.)**.

Ove se ne ravvisi la necessità, la scuola potrà avvalersi della consulenza o dell'intervento di personale tecnico esterno all'ambito scolastico.

Di seguito vengono indicate le funzioni svolte in relazione alla presente e-policy dalle varie figure, già presenti o da creare, interne all'Istituto.

1. **GESTIONE CREDENZIALI PER L'ACCESSO AD INTERNET:**
   - INFANZIA, PRIMARIA E SECONDARIA I GRADO: Segreteria Amministrativa
   - SECONDARIA II GRADO: E.M. e Coordinatore di Plesso
2. **CONTROLLO INFRASTRUTTURA E STRUMENTAZIONE TIC**: E.M.
3. **VERIFICA APPLICAZIONE POLICY**: E.M. e Referente di Plesso
4. **AGGIORNAMENTO POLICY**: E.M., membri del Team Innovazione Digitale, Coordinatori di Plesso, Dirigente Scolastico
5. **FORMAZIONE E CURRICOLO:** membri del Team Innovazione Digitale; Proff. Referenti Progetto Generazioni Connesse
6. **RILEVAZIONE E GESTIONE DEI CASI:** Referente di Istituto per le iniziative contro il Bullismo e cyberbullismo, Coordinatori delle classi coinvolte, Dirigente Scolastico

## CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALLA COMUNITÀ SCOLASTICA

Il presente documento sarà inserito e liberamente consultabile sul sito Internet dell'Istituto.

Verranno effettuate apposite comunicazioni per docenti e famiglie attraverso il Registro Elettronico e, per le altre figure interessate come il Coordinatore di Plesso, l' E-policy Manager, l' Animatore Digitale, attraverso canali specifici;

Il documento verrà illustrato agli studenti all'inizio di ogni anno scolastico.

## GESTIONE DELLE INFRAZIONI ALLA POLICY

Di seguito vengono elencate le varie tipologie di possibili **infrazioni alle regole previste dal vigente regolamento di istituto** (che qui si richiama) con le relative modalità di gestione.

1. *Mancata applicazione delle regole di condotta nel laboratorio di informatica da parte degli studenti;*
2. *Utilizzo improprio o senza consenso delle attrezzature informatiche da parte degli studenti;*
3. *Utilizzo improprio di devices personali da parte degli studenti;*
4. *Mancata applicazione delle regole nell'utilizzo del laboratorio di informatica da parte dei docenti;*
5. *Mancata applicazione delle misure previste per la protezione dell'infrastruttura informatica;*

**Per i punti 1,2,3**: applicazione sanzioni previste dal Regolamento d'Istituto

**Per i punti 4,5**: immediata segnalazione all' E. M. o al Referente di Plesso

## AGGIORNAMENTO DELLA POLICY

L'aggiornamento della policy sarà effettuato periodicamente dall'E.M. (nel caso siano più di uno le decisioni andranno concordaTe) previo parere dei membri del Team per l'Innovazione Digitale, dei Coordinatori di Plesso e sotto la supervisione del Dirigente Scolastico.

## INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI

Il presente regolamento è coerente con quanto stabilito dal **REGOLAMENTO DI ISTITUTO**.

Inoltre, al fine di aumentare il livello di sicurezza nell'utilizzo della strumentazione ICT, si propongono di seguito delle integrazioni e aggiunte al Regolamento vigente.

### PROPOSTA DI INTEGRAZIONE ART. 26 DEL REGOLAMENTO DI ISTITUTO- DIVIETI

Aggiungere i seguenti divieti validi per tutti gli **studenti** della scuola **PRIMARIA e SECONDARIA:**

- *Divieto di utilizzare pendrive su tutti i computer della scuola (da sostituire, se necessario, con l'utilizzo di strumenti di archiviazione remota).*
- *Divieto di utilizzare le LIM o altre apparecchiature informatiche senza l'esplicito consenso del docente.*
- *Divieto di fare foto o registrazioni audio/video e di diffonderle, senza l'autorizzazione del docente, anche se a fini inerenti l'attività didattica, senza il consenso di tutti i soggetti ripresi o registrati.*

### PROPOSTA DI INTEGRAZIONE DEL REGOLAMENTO DEL LABORATORIO DI INFORMATICA DELLA SCUOLA SECONDARIA DI PRIMO E SECONDO GRADO

**Si propone la seguente integrazione finale al punto 1) :**

**"***Il docente è tenuto a compilare ad inizio anno scolastico un apposito modulo* annotando *per ogni gruppo di alunni la postazione occupata o il tablet utilizzato (stabiliti per ogni classe ad inizio anno scolastico), registrando in corso d'anno eventuali variazioni rispetto alla disposizione iniziale. Gli studenti sono tenuti a segnalare al docente eventuali cambi di*

*postazione o tablet (per esigenze tecniche o didattiche) prima dell'inizio dell'attività didattica.*"

**Si propone la seguente integrazione finale al punto 17) :**

"*Si raccomanda l'archiviazione remota attraverso:*

- ***LMS*** **(Nota 1)** *nel caso di file personali come test, verifiche, esercizi da condividere con i docenti*
- ***Cloud Storage*** **(Nota 2)** *nel caso di semplice archiviazione di file personali o materiale di studio non pubblicato sulle precedenti piattaforme o sul web. Sarà cura del docente di informatica assicurarsi che* ***per tutti gli studenti venga creato un account personale*** *su almeno una di tali piattaforme.*"

*Nota 1) ES. EDMODO, WESCHOOL, GOOGLE CLASSROOM ;*

*Nota 2) ES. GOOGLE DRIVE, DROPBOX, MICROSOFT ONEDRIVE*

## ULTERIORI INTEGRAZIONI AL REGOLAMENTO DI ISTITUTO

1. Integrare il **Regolamento dell'Aula di Informatica della PRIMARIA**, già redatto, nel Regolamento di Istituto
2. **Si propone di integrare il Regolamento** in merito all'utilizzo di **devices personali degli studenti**, così come descritto nel paragrafo Strumentazione Personale, cui si rimanda.

# FORMAZIONE E CURRICOLO

## CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

A partire dall'anno scolastico 2017-18, per alcune classi della Scuola Primaria e Secondaria di I e II Grado verrà predisposto, in via sperimentale, un percorso formativo specifico orientato all'acquisizione di:

- nozioni base di sicurezza informatica (dati sensibili, virus, hackers, botnet, social hacking, pishing, false identità…);
- **conoscenza dei pericoli e delle insidie della rete (cyberbullismo, sexting, adescamento);**
- ricerca di informazioni in rete e valutazione della loro attendibilità;
- creazione e utilizzo di un account google per l'invio di mail, utilizzo di **Google Drive, Dropbox, Microsoft OneDrive** per l'archiviazione di file e di **Google Documenti, iCloud** per la redazione di documenti;
- nozioni di base di informatica (istruzione, alternativa, ciclo) attraverso il linguaggio Blocky.

Il percorso, diviso in moduli, verrà calibrato sulla base dell'ordine e del grado di scuola, realizzato in modalità mista con lezioni in aula e con utilizzo di piattaforme di e-learning; le competenze acquisite dagli studenti, per ogni modulo, verranno valutate attraverso test e prove pratiche.

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

Al fine di garantire la formazione dei docenti, saranno organizzati:

- **Incontri periodici di aggiornamento** (Workshop organizzati dal Team Innovazione Digitale);
- **Incontri con esperti;**
- **Siti web dedicati : SCUOLA DIGITALE , DIDATTICARISORSE.**

## FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

Verrà predisposto, a partire dall'anno scolastico 2017-2018, un breve corso online sui seguenti temi:

- nozioni base di sicurezza informatica (dati sensibili, virus, hackers, botnet, social hacking, pishing, false identità…);
- **conoscenza dei pericoli e delle insidie della rete (cyberbullismo, sexting, adescamento);**
- e-safety policy;
- selezione di risorse disponibili per la formazione e l'attività didattica;

Al termine del corso le competenze raggiunte verranno valutate attraverso un test.

## SENSIBILIZZAZIONE DELLE FAMIGLIE

Al fine di sensibilizzare i genitori sarà reso disponibile online del materiale informativo relativo alla sicurezza informatica, analogo a quello delineato sopra per i docenti (ma limitato ai primi 3 punti) e un test (facoltativo), in maniera da sensibilizzare le famiglie sulle tematiche affrontate e le iniziative intraprese dalla scuola.

# GESTIONE INFRASTRUTTURA E STRUMENTAZIONE ICT DELLA SCUOLA

Di seguito vengono illustrate per i vari ordini e gradi di scuola le **misure predisposte** e le **misure da implementare** per quanto riguarda:

- l'accesso ad Internet
- la gestione degli accessi

### ACCESSO AD INTERNET

Le misure predisposte e quelle in programma hanno lo scopo di garantire un accesso costante, veloce e sicuro alla rete, in tutti i locali dell'Istituto, per esigenze funzionali all'attività didattica o ad essa connesse, quali la formazione del personale, le comunicazioni interne, l'archiviazione e la condivisione di risorse, la realizzazione di progetti e iniziative promosse in ambito scolastico.

Le suddette misure hanno anche lo scopo di impedire un utilizzo improprio della connessione da parte degli studenti.

Per tutte le sedi dell'Istituto è auspicabile una verifica periodica della funzionalità dell'impianto WI-FI.

Si precisa che con il termine DEVICES ALUNNI si intendono SMARTPHONE, TABLET, SMARTWATCH, NOTEBOOK.

## INFANZIA

| Misure Predisposte |
|---|

- **WIFI:**
  - **sistema di controllo degli accessi e limite del traffico settimanale per singolo utente**

## PRIMARIA E SECONDARIA I GRADO

### Misure Predisposte

- WIFI:
  - sistema di controllo degli accessi e limite del traffico settimanale per singolo utente
  - account personali per studenti e docenti
- DEVICES ALUNNI:
  - raccomandazione di non portarli a scuola per la PRIMARIA
  - consentiti per finalità  didattiche concordate con il docente, altrimenti spenti

### Misure da Implementare

- WIFI:
  - Spegnimento fuori dall'orario di servizio o limitazione oraria account studenti
  - Ampliamento della banda (sottoscrizione di un contratto separato per la linea ADSL)
- DEVICES ALUNNI:
  - Consegna al docente all'ingresso in aula o all'inizio della lezione

## SECONDARIA II GRADO

### Misure Predisposte

- WIFI:
  - al momento solo i docenti possono accedere al WIFI
- DEVICES ALUNNI:
  - consentiti per finalità  didattiche concordate con il docente, altrimenti spenti

### Misure da Implementare

- WIFI:
  - Ampliamento della banda e della copertura
- MONITORAGGIO SITI VISITATI
- DEVICES ALUNNI:
  - Consegna al docente all'ingresso in aula o all'inizio della lezione

**GESTIONE ACCESSI**

La gestione degli accessi all'infrastruttura e alla strumentazione ICT della scuola è fondamentale per tutelare la strumentazione stessa e soprattutto la **privacy** e la **sicurezza degli utenti.**

Anche in questo caso, come nel precedente, è fondamentale la formazione degli utenti.

E' appena il caso di ricordare che un computer usato normalmente dai docenti, se non protetto da password, può esporre la scuola al furto di tutte le password digitate, e pertanto alla totale compromissione del Registro Elettronico e al furto dei dati personali di tutti i docenti del plesso (nel caso in cui i docenti utilizzino anche solo occasionalmente tali computer oppure le medesime password per accedere alle caselle e-mail personali, a siti istituzionali o finanziari).

Inoltre gli **studenti** potrebbero involontariamente **compromettere il funzionamento dei computer** attraverso pendrive infette causando il **furto dei dati personali degli studenti e dei docenti che li utilizzano**.

**La compromissione dei computer di segreteria** avrebbe effetti ancora più gravi in termini di **furto dei dati personali dell'intero personale scolastico, degli studenti e delle famiglie.**

Per questo si raccomanda di adottare le misure di seguito elencate, che hanno lo scopo di garantire un **LIVELLO MINIMO** di sicurezza e di privacy per gli utenti, siano essi docenti o studenti, che utilizzano tale strumentazione. Risulta determinante anche la verifica periodica della loro applicazione.

## INFANZIA

| **Misure Predisposte** |
|---|

- AULA MULTIMEDIALE:
  - accesso consentito solo in presenza di docenti

| **Misure da Implementare** |
|---|

- AULETTA MULTIMEDIALE:
  - account **Docente**(senza possibilità di installare applicazioni o modificare le impostazioni di configurazione) protetto da password
  - account **Amministratore** riservato all' E.M. protetto da password

## Misure Predisposte

- AULA MULTIMEDIALE/LABORATORIO DI INFORMATICA:
  - accesso consentito solo in presenza di docenti
  - registro presenze di laboratorio (classe e docente)
  - SOLO SECONDARIA II GRADO: registro firme per ogni postazione
  - SOLO PRIMARIA: **postazioni/tablet assegnati** ai vari studenti ad inizio anno

## Misure da Implementare

- AULA MULTIMEDIALE/LABORATORIO DI INFORMATICA:
  - account **Studente di classe o sezione** protetto da password e senza possibilità di installare applicazioni o modificare le impostazioni di configurazione
  - account **Docente** protetto da password e senza possibilità di installare applicazioni o modificare le impostazioni di configurazione
  - account **Amministratore** riservato all' E.M. protetto da password
  - utilizzo di sistemi di **archiviazione remota** dei file attraverso account personali (diversi per ogni singolo studente o docente)
  - utilizzo delle **classi virtuali** per l'archiviazione di file di classe (attraverso piattaforme come Edmodo, WeSchool, Google Classroom )
  - **blocco** dei supporti esterni di memoria per account Studenti e Docenti
  - **postazioni/tablet assegnati** ai vari studenti ad inizio anno(anche per la Scuola Secondaria) con **modulo per annotare eventuali variazioni**

- AULE, SALA DOCENTI, ALTRI LOCALI:
  - account **Amministratore** riservato all' E.M. protetto da password
  - account **Docente** protetto da password e senza possibilità di installare applicazioni o modificare le impostazioni di configurazione
  - **divieto** di utilizzare **pen drive**

REGISTRO ACCOUNT:

- Predisposizione di un REGISTRO dove siano riportate t**utte le credenziali di accesso per gli account Amministratore**(per tutti i plessi scolastici) e **obbligo per l'E.M.di aggiornarlo**
- Il registro deve essere **custodito in forma cartacea dalla segreteria** in un apposita cartella
- Le credenziali di accesso per ogni singolo plesso dovranno inoltre essere comunicate **al Referente di Plesso** qualora questo non svolga la funzione di E.M.

## ANTIVIRUS

Allo scopo di impedire l'installazione involontaria di malware e al fine di **tutelare la privacy del personale scolastico e degli studenti**, tutti i computer della scuola devono essere dotati di Antivirus e deve essere posta particolare attenzione acchè questi siano costantemente aggiornati.

La rilevazione di malware da parte degli antivirus installati deve essere comunicata ai docenti e al personale autorizzato, in maniera da gestire eventuali minacce in modo appropriato e tempestivo.

A tal fine è necessario che il **personale scolastico** (in particolare docenti e personale di segreteria) **e gli studenti siano consapevoli dei rischi derivanti dai malware e dei limiti dei software utilizzati per la loro rilevazione ed eventuale rimozione**.

E' indispensabile inoltre **limitare l'utilizzo delle pendrive** a favore di soluzioni di archiviazione e condivisione remota o a favore dell'utilizzo della posta elettronica.

Si rende pertanto necessaria una preventiva opera di formazione che è inclusa nel **curriculum digitale delle competenze,** previsto dalla presente policy.

## STRUMENTAZIONE

Al fine di garantire un utilizzo efficace delle TIC all'interno dell'attività didattica è necessario avere a disposizione una strumentazione hardware e software adeguata.

Si prevede, dunque, la predisposizione di un modulo per la richiesta di strumentazione, l'aggiornamento di quella esistente e la segnalazione di malfunzionamenti.

Tale modulo avrà come destinatario l'E.M. che provvederà a inoltrarla alle figure competenti.

## SITI WEB DELLA SCUOLA

- **Sito ufficiale**: ISTITUTOMNICOMPRENSIVOTRIVENTO

Oltre al suddetto sito istituzionale, vi è una serie di siti collegati alle attività dell'Istituto, i quali si riportano di seguito:

- **Siti contenti risorse per favorire l'utilizzo delle TIC nella didattica e l'aggiornamento del personale docente**:
  - SCUOLA DIGITALE

- DIDATTICARISORSE

- **Altro:**
  - **Liceo** (blog): LICEOTRIVENTOLIVE
  - **Scuola Primaria** (blog, homepage dei docenti, siti realizzati dagli studenti): LINKS

## TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI

*"Ogni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza."*

(DICHIARAZIONE DEI DIRITTI IN INTERNET - ART. 5)

In fase di iscrizione degli alunni, i genitori sottoscrivono un'informativa sul trattamento dei dati personali, in ottemperanza all'art. 13 D.L. 30 giugno 2013 , n. 196.

Viene richiesta l'autorizzazione degli alunni, o dei genitori in caso di alunni minorenni, per la realizzazione, raccolta, conservazione, divulgazione e utilizzo da parte dell'Istituto, per scopo esclusivamente didattico-educativo, di foto, video e altro materiale audiovisivo, contenenti l'immagine, il nome, la voce degli alunni.

La stessa autorizzazione viene richiesta da parte dell'Istituto anche a soggetti terzi per il trattamento di dati personali ove ve ne sia necessità.

L'accesso ai dati riportati nel Registro Elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori, tramite la consegna di una password di accesso.

Come delineato in precedenza, gli studenti vengono sensibilizzati nei confronti del problema della protezione dei dati personali attraverso una serie di attività, tra le quali figurano, in particolare, incontri con esperti di sicurezza informatica e diffusione di materiale informativo. La scuola prevede di rafforzare questa attività di sensibilizzazione, nei prossimi anni, attraverso il **CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI.**

Per quanto riguarda le regole principali da seguire per la tutela della privacy, si fa riferimento al VADEMECUM del **Garante per la privacy.**

# STRUMENTAZIONE PERSONALE

## DEVICES STUDENTI

Ai sensi del Regolamento di Istituto, art. 25 **"E' vietato a tutti gli studenti l'uso dei telefoni cellulari all'interno dell'Istituto e pertanto questi dovranno essere spenti. Gli studenti che venissero sorpresi all'interno dell'Istituto ad usare il telefono cellulare subiranno la requisizione temporanea dello stesso."**

Secondo la Direttiva Ministeriale del 15 marzo 2007**,** oltre all'obbligo di introdurre sanzioni disciplinari al riguardo (già previste nel Regolamento d'Istituto vigente), gli Istituti hanno la facoltà di introdurre misure organizzative idonee a prevenire, durante le attività didattiche, un utilizzo scorretto del telefonino.

A tal fine, si ritiene utile proporre la seguente integrazione al Regolamento di Istituto:

## PROPOSTA DI MODIFICA E INTEGRAZIONE ART.25

**Modificare il titolo in "Uso del telefono e di devices personali"**

**Nel testo vigente laddove compare "telefono cellulare" aggiungere "e devices personali"**

**Modificare l'ultimo comma nel seguente modo:**

Dopo la parola "*spenti*" aggiungere "*e, all'ingresso in aula, depositati. I cellulari/device personali verranno custoditi secondo modalità decise dal consiglio di classe, e verranno riconsegnati a ciascun alunno al termine delle lezioni. Sono ammesse deroghe, con l'esplicita autorizzazione dei docenti,* ***al suddetto regolamento, nel caso in cui smartphone e tablet siano funzionali all'attività didattica o necessari per esigenze di comunicazione con*** *la famiglia, dettate da ragioni di particolare urgenza e o gravità*".

# PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

**Prevenzione**

**Secondo le disposizioni della Legge "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"** in ogni Istituto sarà individuato un insegnante referente contro il bullismo e cyberbullismo; nell'Istituto IOT tale figura è presente, in quanto già individuata dalla Dirigenza.

**Sempre ai sensi della predetta legge** e quindi al fine di contrastare i pericoli legati ad un utilizzo non consapevole di Internet e dei nuovi media, si ritiene fondamentale la **sensibilizzazione e** la **formazione** di **studenti, docenti e famiglie** e pertanto l'Istituto prevede, tra le varie attività:

- **Incontri di informazione e sensibilizzazione con esperti,** sui temi legati sia alla sicurezza informatica che alle tematiche di carattere sociale connesse all'utilizzo di social network
- **Diffusione di materiale informativo**
- **Coinvolgimento delle famiglie e dei docenti nella redazione e aggiornamento policy**
- **Coinvolgimento delle famiglie, dei docenti e degli studenti nella valutazione delle iniziative prese** nell'ambito di tali tematiche

Per quanto concerne il terzo e quarto punto, le modalità scelte consistono in incontri e questionari online, per raccogliere opinioni e indicazioni da parte del numero più ampio possibile di persone.

Per quanto riguarda i primi due punti si ritiene opportuno sensibilizzare i genitori sui pericoli legati all'utilizzo dei gruppi WhatsApp creati spontaneamente dagli studenti nell'ambito della classe. Tali gruppi, infatti, di frequente sono il "luogo" in cui si verificano episodi di cyber-bullismo. Pertanto, si considera utile raccomandare ai genitori di monitorare regolarmente le conversazioni che avvengono su tali gruppi, anche alla luce delle ricadute legali connesse all'utilizzo improprio di tali strumenti.

**Rilevazione**

Sul sito dell'Istituto, precisamente sulla homepage, cliccando sul banner "UN NODO BLU - SEGNALA IL TUO DISAGIO" è possibile accedere a moduli per la segnalazione di casi di bullismo o cyberbullismo, tentativi di adescamento on line, casi di sexting e comportamenti scorretti in genere. Le segnalazioni possono riguardare **episodi personali o che riguardino terze persone, di cui si abbia conoscenza diretta, oppure indiretta perché riferiti da altri** (ad esempio i genitori possono segnalare vicende riferite dai propri figli e riguardanti i loro compagni).

Nel modulo vengono richieste informazioni utili ad identificare i soggetti coinvolti nonché, ovviamente, una sintetica descrizione dei fatti. La segnalazione può essere fatta anche in forma anonima e può provenire tanto dagli **studenti** che dai **genitori** o dai **docenti**.

La comunicazione così effettuata viene automaticamente inviata su una casella di posta elettronica dedicata, **controllata e gestita dal Referente di Istituto per le iniziative contro il Bullismo e Cyberbullismo.**

**Gestione**

Al ricevimento della segnalazione, il Referente di Istituto per le iniziative contro il Bullismo e il Cyberbullismo informa il Dirigente, nonché il Professore coordinatore delle classi frequentate dalle persone coinvolte.

Essi, dopo essersi accertati della veridicità del fatto, INFORMANO SUBITO LE FAMIGLIE DEI SOGGETTI COINVOLTI e decidono la modalità di gestione del caso, che prevederà il loro intervento, unito a quello delle famiglie ed eventualmente, a seconda della tipologia e gravità dello stesso, il coinvolgimento, in via esclusiva o cumulativa, delle seguenti componenti scolastiche e territoriali:

- SERVIZI SOCIALI DEL TERRITORIO;
- CONSIGLIO DI CLASSE;
- RAPPRESENTANTI DI CLASSE DEGLI STUDENTI.

In caso di violazione del Regolamento d'Istituto, si procederà all'applicazione delle relative sanzioni in esso previste. Nei casi in cui gli episodi segnalati configurino ipotesi di reato perseguibili d'ufficio, verrà sporta denuncia presso l'Autorità Giudiziaria o alle Forze dell'Ordine competenti. Il personale scolastico/amministrativo, in quanto personale incaricato di pubblico servizio, è infatti tenuto a denunciare la notizia di ogni reato procedibile d'ufficio di cui viene a conoscenza nell'esercizio o a causa delle funzioni o del servizio (art. 331 cod.proc.pen.).

Tutti i casi segnalati e trattati vengono annotati su apposito registro (Diario di Bordo).

TRIVENTO, 8 giugno 2017

Il Dirigente Scolastico
(Prof.ssa Maria Maddalena Chimisso)