



Ministero dell'Istruzione Università e Ricerca
Ufficio Scolastico Regionale per la Campania
ISTITUTO STATALE COMPRESIVO "Can. SAMUELE FALCO"
Corso Trieste, 324 cap 84018 SCAFATI (SA)

Mail: saic88200x@istruzione.it - PEC: saic88200x@pec.istruzione.it
TEL . 081.8504452 – FAX 0818563815- C.F. 80034160657 - www.icfalcoscafati.gov.it

Prot. n. 3849-04-05

Scafati, 06/12/2017

E-Safety Policy

1. Introduzione

1. Scopo della *policy*.
2. Ruoli e responsabilità (*che cosa ci si aspetta da tutti gli attori della comunità scolastica*).
3. Condivisione e comunicazione della *policy* all'intera comunità scolastica.
4. Gestione delle infrazioni alla *policy*.
5. Integrazione della *policy* con Regolamenti esistenti.

2. Formazione e Curricolo

1. Curricolo sulle competenze digitali per la componente studentesca.
2. Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
3. Formazione del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

1. Accesso ad internet: filtri, antivirus e sulla navigazione.
2. Gestione accessi (password, backup, ecc.).
3. E-mail.
4. Sito web della scuola.
5. Social network.
6. Protezione dei dati personali.

4. Strumentazione personale

1. Per la componente studentesca: gestione degli strumenti personali - cellulari, tablet ecc.
2. Per il corpo docente e per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

Rischi
Azioni

Rilevazione

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

Gestione dei casi

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

1. INTRODUZIONE

1.1 Scopo della *policy*.

Questa *policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.

In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di *buone pratiche* quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica. Questo è il caso degli episodi di cyber-bullismo come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa.

L'I.C. "Can. Samuele Falco" accoglie minori "*nativi digitali*" che, fin dall'infanzia, sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

La scuola opera in stretto collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber-bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

1.2 Ruoli e responsabilità (*che cosa ci si aspetta da tutti gli attori della comunità scolastica*).

Dirigente Scolastico

È responsabile della presentazione -entro la fine dell'a.s. 2017/18- di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti; deve anche valutare l'efficacia della politica e monitorarne/indirizzarne l'attuazione, anche in collaborazione con personale scolastico, enti locali e *stakeholder* territoriali. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.

Animatore digitale e Referente Sito Web

Cura la redazione e la revisione annuale della *policy* sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola. Si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Personale docente, con particolare riferimento ai Coordinatori dei Consigli di Classe

I docenti sono tenuti ad assicurare di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente *policy*;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- integrare i problemi di sicurezza informatica in tutti gli aspetti del curriculum di studi e in altre attività extracurricolari;

- far comprendere e mettere in pratica alla componente studentesca le regole di comportamento relative alla sicurezza informatica;
- far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

Personale ATA

Il personale ATA è tenuto ad assicurare di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente *policy*;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;

Componente studentesca

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa *policy*. In particolare sono tenuti a:

- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali; capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso incontri con la Polizia municipale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di *e- safety* e a seguire le linee guida sull'uso appropriato di:

- immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli nella scuola (dove ciò è consentito).

1.3 Condivisione e comunicazione della *policy* all'intera comunità scolastica.

Per evitare che l'adozione di questa *policy* rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:

Per il corpo docente, discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse della *policy*.

Per la componente studentesca, la discussione in classe della *policy* nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime; l'inserimento di un estratto di questo documento nel diario scolastico e in particolare dei comportamenti da attuare in caso di bisogno.

Per i genitori, l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

1.4 Gestione delle infrazioni della *policy*.

Le infrazioni alla *policy* possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- Minaccia*, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 cod. pen.);
- Induzione alla prostituzione minorile* (art. 600bis);
- Pedopornografia* (art. 600ter);
- Corruzione di minorenni* (art. 609quiquies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

Nel caso in cui le infrazioni della *policy* violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

1.5 Integrazione della *policy* con Regolamenti esistenti.

La *Policy* è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") dai Regolamenti vigenti (di Istituto, interno degli alunni, delle visite didattiche) e dal Patto di Corresponsabilità.

Il Dirigente Scolastico è responsabile dell'implementazione della *Policy* all'interno dell'Istituto. L'Animatore Digitale (insieme al Team dell'innovazione digitale), i Responsabili di Plesso ed il Referente per il Bullismo e il Cyberbullismo, in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento.

La presente *policy* è allegata in appendice al Patto di Corresponsabilità e/o al Regolamento di Istituto.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per la componente studentesca.

Le TIC e Internet sono un elemento essenziale nella vita del XXI secolo. La scuola ha il dovere di fornire alla componente studentesca l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale. L'uso delle TIC va inserito pertanto nel curricolo sia a livello disciplinare sia a livello interdisciplinare.

In particolare il curricolo dovrà essere strutturato per prevedere di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia per un pubblico più vasto;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

2.2 Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta da docenti dell'Istituto che fanno parte del team digitale, per cui il MIUR prevede opportuni percorsi la cui ricaduta viene annualmente tarata secondo le esigenze formulate dal Collegio Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche.

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.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

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

Data la giovane età degli studenti del nostro istituto è fondamentale fare tutto il possibile per evitare l'esposizione a contenuti inappropriati. Gli alunni non sono mai lasciati soli nelle aule in cui sono presenti dei computer collegati ad internet.

I laboratori dei vari plessi dell'IC. "Falco" sono dotate di antivirus, monitorati e tenuti aggiornati dai responsabili dei laboratori informatici.

3.2 Gestione accessi.

Nei locali della scuola primaria i computer, sia nell'aula informatica che nelle classiche hanno in dotazione un pc portatile, hanno un unico nome utente e password. La connessione alla rete wi-fi è riservata ai docenti per fini didattici ed è accessibile solo dietro identificazione personale.

Nei locali della scuola secondaria tutte le aule sono dotate di pc portatili, collegati alla LIM, cui ha l'accesso ogni docente per la compilazione del registro elettronico e come support alla didattica; ogni docente, inoltre, può accedere ai computer dei laboratori informatici, previa immissione della password da parte del responsabile del laboratorio. La connessione alla rete wi-fi è accessibile dietro identificazione personale ed è disponibile per i docenti e per gli alunni (sotto la supervisione del docente stesso) esclusivamente per fini didattici.

Altre norme sono consultabili nel Regolamento d'Istituto (Capo IX – Regolamento: Utilizzo laboratori – Art.1 Accesso ed utilizzo delle apparecchiature dei laboratori).

3.3 E-mail.

L'Istituto fornisce una casella di posta elettronica @icfalcoscafati.gov.it a tutto il personale docente e ATA e, in alcuni casi legati all'uso di metodologie didattiche quali la *flipped classroom*, a una parte della componente studentesca.

Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo.

Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento, per consentire l'attivazione di protocolli di controllo.

E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

3.4 Sito web della scuola.

Il sito dell'I.C. "Falco" è raggiungibile all'indirizzo <http://www.icfalcoscafati.gov.it/>. Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione.

I dati di contatto sul sito web devono essere: indirizzo della scuola, e-mail e numero di telefono. Solo eccezionalmente, previa richiesta alla scuola, sono utilizzabili le comunicazioni via fax. Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

3.5 Social network.

In diverse classi della scuola secondaria è diffuso l'utilizzo della piattaforma didattica Edmodo e We School, diffuse anche le applicazioni Padlet e Sway, mentre nelle scuole primarie alcune classi intendono sperimentare l'utilizzo di Google Classroom.

La scuola è in grado di controllare l'accesso ai siti di social networking attraverso i *log* del *proxy server*; nella pratica didattica si cerca di educare la componente studentesca al loro uso sicuro. Per esempio a ogni utente sarà consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione.

La componente studentesca non deve pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico. Alunne/alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio.

3.6 Registro elettronico.

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 consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

3.7 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.

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 per esporli anche in sedi diverse da quelle dell'Istituto, quali pubblicazioni in formato digitale e siti web. 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.

In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori.

In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori della Scuola secondaria di primo grado tramite l'invio di una password di accesso strettamente personale.

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca.

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni; nella scuola secondaria di primo grado all'ingresso in aula, dopo l'appello, la componente studentesca deposita telefoni e altri dispositivi dentro un contenitore appositamente collocato in classe, visibile a tutti.

Individui con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia nell'armadietto della classe.

Giochi e console, tra cui la Sony Playstation, Microsoft Xbox e similari, che possono avere accesso a Internet non filtrato, non sono consentiti nemmeno se custoditi dentro l'armadietto dell'aula. Saranno requisiti dal docente che ravvisa l'infrazione, depositati nella

cassaforte della segreteria e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

4.2 Per il personale docente/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.

La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni). L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (floppy disk, chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe.

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.

I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi dell'utilizzo consapevole di internet e a formarsi su queste tematiche.

I genitori si impegnano a prendere visione della E-safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.

Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.

Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting), la scuola si affida a consulenti esterni per organizzare incontri informativi rivolti agli alunni.

Rilevazione

Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyberbullismo (caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network), ma anche usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni...).

I docenti di classe informano il referente per il bullismo/cyberbullismo. Il referente informa il Dirigente Scolastico, il quale procede ad informare le famiglie.

Gestione dei casi

Per un'efficace gestione dei casi, i docenti si attengono alle modalità illustrate nello schema messo a disposizione da Generazioni Connesse (allegato).

RISCHI	AZIONI
Adescamento online (<i>grooming</i>)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, <i>shopping</i> o <i>gambling</i> online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curriculum di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
<i>Sexting</i> e pedopornografia.	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curriculum di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

Scafati, 30 novembre 2017

Il Dirigente Scolastico
Domenico Coppola

Documento firmato digitalmente ai sensi del c.d. CAD e normativa connessa

