ISTITUTO COMPRENSIVO "ERNESTO BORRELLI"

Scuola Infanzia Primaria e Secondaria di Primo Grado ad Indirizzo Musicale

VIA SCAFATI 10 - 80050 SANTA MARIA LA CARITÀ (NA)

Cod. Mecc. NAIC8B6005 - Cod. Fisc. 82008890632 Cod. Univoco UFAL3G

Tel./Fax 081/8741505

@mail naic8b6005@istruzione.it e naic8b6005@pec.istruzione.it

Sito web www.icborrelli.gov.it/portale

DOCUMENTO DI E-SAFETY POLICY

Anno Scolastico 2017/18

Indice

1. Introduzione

Nell'anno scolastico 2017-18 l'Istituto ha aderito al Progetto "Generazioni Connesse", co-finanziato dalla Commissione Europea nell'ambito del programma "Connecting Europe Facility" (CEF), programma attraverso il quale la Commissione promuove strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, promuovendone un uso positivo e consapevole. Il progetto si inserisce nel quadro delle attività svolte dal MIUR nell'ambito dell'attuazione del Piano Nazionale Scuola Digitale e consta di diverse azioni, tra le quali la produzione di un *documento di e-policy*, che fornisca gli strumenti necessari sia a promuovere un uso corretto di internet e delle tecnologie digitali sia a prevenire, riconoscere e gestire eventuali situazioni problematiche.

1.a Scopo della policy

La Policy di e-safety (e-policy) è un documento programmatico autoprodotto dalla scuola volto a descrivere:

- ✓ il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica
- ✓ le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (TIC) in ambiente scolastico
- ✓ le misure per la prevenzione, la rilevazione e la gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1.b Ruoli e Responsabilità

Di seguito vengono specificate le responsabilità di tutti i componenti della comunità scolastica.

Dirigente Scolastico

- ✓ Garantire che la scuola utilizzi un Internet Service filtrato
- ✓ Garantire che tutti i docenti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, dell'utilizzo positivo e responsabile delle TIC
- ✓ Seguire le procedure previste dalle norme, coordinandosi con le autorità locali e con le agenzie competenti, per gestire casi di episodi di cyberbullismo, di grooming, ecc. in cui sono coinvolti gli alunni.

Animatore Digitale

- ✓ Stimolare la formazione interna negli ambiti di sviluppo della scuola digitale e fornire consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi
- ✓ Aggiornare il sito web della scuola
- ✓ Coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la scuola digitale
- ✓ Pubblicare sul sito web dell'Istituto il documento integrale E-Safety Policy e una presentazione in Power Point con slide semplificative
- ✓ Garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati

Direttore dei Servizi Generali e Amministrativi

- ✓ Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni
- ✓ Garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, registro elettronico, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni

Docenti

- ✓ Informarsi/aggiornarsi sulle problematiche attinenti la sicurezza nell'utilizzo delle tecnologie digitali e della Rete e sulla politica di sicurezza adottata dalla scuola, rispettandone il Regolamento.
- ✓ Garantire che le modalità di utilizzo corretto e sicuro delle TIC e della Rete siano integrate nelle attività didattiche ed educative.
- ✓ Garantire che gli alunni condividano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e della Rete.
- ✓ Assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla Rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore.
- ✓ Garantire che le comunicazioni digitali con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi ufficiali.
- ✓ Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente.
- ✓ Controllare l'uso delle tecnologie digitali (dispositivi mobili, macchine fotografiche, ecc.) da parte degli alunni durante le lezioni e ogni altra attività scolastica, ove consentito.
- ✓ Nelle lezioni in cui è programmato l'utilizzo della Rete, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche in Rete siano trovati e trattati solo materiali idonei.
- ✓ Comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo.
- ✓ Segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo, ovvero esigenza di carattere informativo, all'Animatore Digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC.
- ✓ Segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o della Rete, per l'adozione delle procedure previste dalle norme.

Alunni

- ✓ Conoscere e comprendere la E-Safety Policy della scuola.
- ✓ Essere responsabili nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti.
- ✓ Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore.
- ✓ Comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi.
- ✓ Adottare condotte rispettose degli altri anche quando si comunica in Rete.

- ✓ Esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o della Rete ai docenti e ai genitori.
- ✓ Comprendere l'importanza di segnalare abusi o l'uso improprio o l'accesso a materiali inappropriati.
- ✓ Conoscere quali azioni intraprendere se loro o qualche conoscente si sente preoccupato o vulnerabile quando utilizza la tecnologia on-line

Genitori

- ✓ Conoscere e accettare la E-Safety Policy della scuola
- ✓ Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica
- ✓ Seguire i propri figli nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e della Rete.
- ✓ Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi scaturiti da un uso non responsabile o pericoloso delle tecnologie digitali o della Rete.
- ✓ Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno della Rete e del telefonino in generale.

1.c Condivisione e comunicazione della Policy all'intera comunità scolastica

Il documento di e-policy dell'istituto verrà condiviso e comunicato all'intera comunità scolastica (studenti, genitori, personale) attraverso vari canali

- ✓ Discussione negli Organi collegiali (Consigli di classe/interclasse/intersezione, Collegio dei docenti) e comunicazione formale a tutto il personale.
- ✓ Implementazione di attività didattiche sulla e-Safety per promuovere un uso consapevole e critico da parte degli alunni delle tecnologie digitali e di Internet.
- ✓ Implementazione di attività didattiche per favorire l'acquisizione di procedure e competenze tecnico-operative e di corrette norme comportamentali (Netiquette).
- ✓ Lettura in classe del documento di e-policy adottato dall'Istituto.
- ✓ Pubblicazione sul sito web dell'Istituto del documento integrale e di una presentazione in PPT con slide semplificative.
- ✓ Pubblicazione delle regole per la sicurezza on-line in tutte le aule o laboratori con accesso della Rete e sul sito web dell'Istituto.
- ✓ Dichiarazione di responsabilità per l'accesso ad internet nella rete di istituto e per l'utilizzo dei dispositivi elettronici sottoscritto dalle famiglie all'inizio del primo anno (Allegato n.1).
- ✓ Condivisione sul sito web della scuola di materiale e strumenti utili per la didattica da utilizzare con gli studenti.
- ✓ Attività di sensibilizzazione al tema della sicurezza nell'uso delle TIC e della Rete in occasione degli incontri Scuola-Famiglia, assembleari, collegiali e individuali.
- ✓ Divulgazione ai genitori di indirizzi-web relativi a risorse utili per lo studio e di siti idonei ed educativi per gli alunni, di sistemi di filtraggio e di attività educative per il tempo libero.

1.d Gestione delle infrazioni alla Policy

Alunni

Il Dirigente Scolastico autorizza i membri del personale ad imporre sanzioni disciplinari per il comportamento inadeguato degli studenti.
Se durante un'attività didattica che prevede l'utilizzo delle TIC o di dispositivi personali gli alunni:

- ✓ giudicano o infastidiscono un compagno oppure impediscono a qualcuno di esprimersi o partecipare
- ✓ inviano foto o altri dati personali senza permesso
- ✓ condividono immagini intime
- ✓ comunicano con sconosciuti
- ✓ si collegano a siti web non indicati dai docenti

verranno applicate i seguenti provvedimenti disciplinari, proporzionati ovviamente alla gravità del comportamento:

- ✓ richiamo verbale
- ✓ richiamo scritto sul registro
- ✓ convocazione dei genitori da parte dei docenti
- ✓ convocazione dei genitori da parte del Dirigente scolastico.

Le eventuali infrazioni saranno gestite con estrema riservatezza e cautela, privilegiando l'ascolto e il riconoscimento dell'errore. Gli studenti che lo richiedano, previa autorizzazione dei genitori, potranno avere dei colloqui con le psicologhe che hanno attivato uno Sportello d'Ascolto all'interno dell'Istituto.
Sono previsti, inoltre, interventi individuali e/o di gruppo per discutere e riflettere sugli eventuali disagi causati dal proprio comportamento, sul rispetto delle regole di convivenza civile, sulla gestione positiva dei conflitti, sulle conseguenze prodotte da eccessiva competitività, sulla promozione di rapporti amicali e solidali, sulla gestione delle emozioni.

Personale scolastico

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso della Rete e procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola.
Il personale scolastico:

- ✓ non deve utilizzare tecnologie e servizi della scuola, d'uso comune con gli alunni, non riconducibili ad attività di insegnamento o al proprio profilo professionale
- ✓ non deve accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola;
- ✓ non deve collegarsi ad Internet a scopi commerciali o di profitto personale e per attività illegali;
- ✓ non deve diffondere virus o altri software malevoli all'interno della rete;
- ✓ non deve scaricare/duplicare/distribuire software o materiali non idonei oppure altri contenuti protetti da diritto d'autore
- ✓ deve garantire un'adeguata protezione dei dati personali e sensibili degli alunni
- ✓ deve custodire in maniera adeguata password assegnate e non deve diffonderle
- ✓ deve intervenire in maniera adeguata nelle situazioni problematiche di cui viene a conoscenza, nella segnalazione al referente, ai genitori e al Dirigente scolastico

Genitori

La scuola convoca i genitori degli alunni che violano le norme della e-policy per concordare le misure educative da attuare, in base alla gravità dei comportamenti dei loro figli. Se tali comportamenti dovessero risultare pericolosi per sé e/o dannosi per gli altri, la scuola comunica le sanzioni disciplinari che ha deciso di applicare.
Per favorire l'uso corretto e responsabile delle TIC i genitori devono:

- ✓ monitorare la navigazione in rete o l'uso del cellulare del proprio figlio
- ✓ essere consapevoli dei pericoli che possono scaturire da un uso scorretto delle TIC
- ✓ non far utilizzare al proprio figlio i dispositivi degli adulti, che potrebbero conservare in memoria materiali o indirizzi non idonei.

1.e Monitoraggio dell'implementazione della Policy e suo aggiornamento

Per adeguare il documento di E-Policy ad eventuali necessità non previste e per verificarne la validità, lo stesso sarà riesaminato annualmente nei mesi di aprile e di maggio oppure anticipatamente, nel momento in cui nascano esigenze particolari.
Tale monitoraggio sarà effettuato dall'Animatore digitale e dai docenti delle classi, tramite questionari e colloqui e sarà finalizzato a rilevare la situazione iniziale e finale delle classi, in relazione all'uso sicuro e responsabile delle tecnologie digitali e della Rete.
L'aggiornamento della policy sarà curato dall'Animatore digitale e approvato dal Dirigente scolastico e dagli Organi collegiali, a seconda degli aspetti considerati**.**

1.f Integrazione della Policy con Regolamenti esistenti

L'Istituto possiede già un Regolamento sui comportamenti da tenere a scuola e un Regolamento del Laboratorio di Informatica. Si rendono necessarie, tuttavia, delle integrazioni relative alla e-Safety Policy, pertanto, ad inizio anno scolastico si provvederà ad aggiornare il Regolamento del Laboratorio d'Informatica con l'inserimento delle seguenti norme:

Regolamento laboratori d'informatica

- ✓ E' vietato l'utilizzo dei dispositivi per i collegamenti alla Rete a scopi commerciali o di profitto personale e per attività illegali
- ✓ E' vietato prelevare o depositare informazioni, applicazioni o documenti che possano in qualsiasi modo arrecare danno a persone, cose o istituzioni
- ✓ E' vietato comunicare ad estranei il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della scuola frequentata
- ✓ E' vietato navigare in siti dai contenuti pornografici, violenti, razzisti
- ✓ E' vietato inviare fotografie proprie o di amici
- ✓ Bisogna rispettare le regole morali e di decenza, evitare atti e comportamenti che possano recare offesa a cose, persone o istituzioni

I docenti che accompagnano gli allievi in laboratorio sono tenuti a controllare che vengano rispettati i divieti sopraelencati e che l'utilizzo delle risorse tecnologiche sia finalizzato agli intenti didattici previsti.

2. Formazione e Curricolo

2.a Curricolo sulle competenze digitali per gli studenti

Dalle "*Indicazioni nazionali e nuovi scenari*", il documento a cura del Comitato Scientifico Nazionale per le Indicazioni Nazionali per il curricolo della scuola dell'infanzia e del primo ciclo di istruzione, si legge:
"La responsabilità è l'atteggiamento che connota la competenza digitale. Solo in minima parte essa è alimentata dalle conoscenze e dalle abilità tecniche, che pure bisogna insegnare. I nostri ragazzi, anche se definiti nativi digitali, spesso non sanno usare le macchine, utilizzare i software fondamentali, fogli di calcolo, elaboratori di testo, navigare in rete per cercare informazioni in modo consapevole. Sono tutte abilità che vanno insegnate. Tuttavia, come suggeriscono anche i documenti europei sulla educazione digitale, le abilità tecniche non bastano. La maggior parte della competenza è costituita dal sapere cercare, scegliere, valutare le informazioni in rete e nella responsabilità nell'uso dei mezzi, per non nuocere a se stessi e agli altri."

La Competenza *digitale* viene inoltre definita all'interno della "Raccomandazione del Parlamento europeo e del Consiglio" del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente (2006/962/CE):
"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".
Chiaramente si tratta di una competenza trasversale a tutte le discipline in quanto in ognuna di esse si ritrovano abilità e conoscenze che fanno capo alla competenza digitale e tutte concorrono a costruirla. Al termine del primo ciclo di istruzione ogni studente:
"Ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo."
Nell'ambito del PNSD questa scuola si attiverà per far acquisire tali competenze attraverso varie proposte ed esperienze:

- ✓ laboratori di Coding
- ✓ corsi di preparazione per la certificazione EiPass Junior
- ✓ gare di informatica
- ✓ attività didattiche che sviluppano la capacità di:
  - utilizzare in modo appropriato materiali digitali per l'apprendimento (motori di ricerca, sistemi di comunicazione mobile, email, social network, ecc)
  - utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini
  - produrre testi, ipertesti, presentazioni multimediali
- ✓ moduli didattici sviluppati con il materiale disponibile sul sito www.generazioniconnesse.it per aiutare gli studenti a :
  - sviluppare strategie per valutare e verificare la correttezza delle informazioni disponibili su internet
  - comprendere l'importanza di non utilizzare comportamenti inappropriati in rete
  - comprendere l'importanza di non diffondere in rete informazioni personali private o informazioni di contatto
  - individuare contenuti web inappropriati
  - essere consapevoli che le amicizie nate on-line potrebbero nascondere identità ben diverse da quelle dichiarate
  - comprendere i danni che possono scaturire dalla pubblicazione di foto o video di altre persone senza il loro permesso
  - saper segnalare eventuali abusi se sono vittime di cyberbullismo, sexting, grooming chiedendo aiuto ai docenti, ai genitori

2b. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

Come specificato nel PTOF, per ciò che concerne la formazione in servizio relativa all'utilizzo e all'integrazione delle TIC nella didattica, l'Istituto ha previsto:

- ✓ Formazione specifica dell'Animatore Digitale e del Team digitale
- ✓ Partecipazione a comunità di pratica in rete con altri animatori del territorio e con la rete nazionale
- ✓ Formazione per i docenti sull'uso di Programmi di utilità on line free per testi cooperativi, presentazioni per attività didattiche con le funzioni di base delle Google

Apps (documenti, fogli di lavoro, presentazioni, moduli, blogger, foto, raccolte) o mappe e programmi di lettura da utilizzare nella didattica inclusiva
- ✓ Sperimentazione e diffusione di metodologie e processi di didattica attiva e collaborativa
- ✓ Utilizzo di cartelle condivise e documenti condivisi di Google Drive per la formulazione e consegna di documentazione: Programmazioni, documenti conclusivi classe terminali, relazioni finali, ecc
- ✓ Corsi per il conseguimento di certificazione Eipass (Eipass 7 moduli user, Eipass LIM, Eipassteacher…)
- ✓ Formazione sull'utilizzo del coding nella didattica

2c. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Relativamente alla formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, sono previsti incontri tematici con esperti durante tutto l'anno scolastico. L'Istituto, inoltre, ha aderito al progetto "Generazioni Connesse" pertanto i docenti possono partecipare online, tramite la piattaforma dedicata, a 4 corsi specifici, all'interno dei quali vengono forniti moduli didattici, materiali di approfondimento, comunità di pratiche, proposte e strumenti operativi per attività da svolgere in classe. Le 4 diverse tematiche disponibili sono:

1. *Uso responsabile e sicurezza on-line*
2. *Educare ai media, educare con i media*
3. *Inclusione e partecipazione a scuola*
4. *Tecnologie a scuola.*

2d. Sensibilizzazione delle famiglie

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento di e-Safety Policy per portare a conoscenza delle famiglie il Regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un uso non corretto di Internet.
L'Istituto, inoltre, promuoverà iniziative specifiche per sensibilizzare le famiglie all'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali:
- ✓ momenti di confronto e discussione sulle dinamiche che si instaurano fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo
- ✓ incontri tematici con esperti
- ✓ diffusione tramite il sito web dell'Istituto di materiale informativo sulle tematiche trattate (guide in formato pdf e video che possono fornire spunti di approfondimento e confronto) e segnalazione di siti di sostegno per i genitori (www.generazioniconnesse.it)

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

3.a Accesso ad internet: filtri antivirus e sulla navigazione

Accesso docenti
Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto attraverso una password personale fornita dall'Istituto.

La connessione Wi-Fi ad Internet dalla scuola è regolata da un meccanismo di autenticazione - autorizzazione:

- ✓ L'accesso può avvenire unicamente da tale dispositivo
- ✓ Il proprietario del dispositivo è l'unico responsabile di tutte le operazioni svolte con esso
- ✓ In caso di furto o smarrimento del dispositivo identificato si deve immediatamente informare il personale tecnico incaricato che ne revocherà l'accesso alla rete.

Accesso studenti

Il Regolamento di Istituto vieta l'uso del cellulare, se non con le eccezioni specificate. Agli studenti in ogni caso, comunque, non è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.

Accesso laboratori e dispositivi della scuola

Tutti i pc dei laboratori informatici (alunni e docenti) sono collegati alla rete con cavo ethernet, ad eccezione di 3 postazioni presenti in quello dei docenti che sono collegate in rete wifi. La scuola, inoltre, dispone di 12 pc Lenovo e 3 pc HP portatili collegati tutti in wi-fi attraverso una password individuale. La scuola dispone di un internet service filtrato per cui a tutta la rete didattica sono applicati dei blocchi che impediscono il collegamento a determinati siti consentendo il collegamento solo a quelli idonei alla didattica.

Sicurezza Rete Lan

Tutti i dispositivi sono dotati di antivirus ma non è garantito alcun servizio di backup, pertanto, chi ha necessità può fare copia dei propri dati su un supporto personale (Pendrive, Hard Disk esterni, o altro). Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione per i dati sensibili (DataBase del registro elettronico)

Sicurezza della rete senza fili (Wireless — WiFi)

L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato da un controller che determina l'accesso degli utenti tramite il riconoscimento del dispositivo utilizzato.

3.b Gestione accessi (password, backup, ecc.)

I docenti che utilizzano il laboratorio d'informatica con i propri alunni registrano il proprio accesso compilando il Registro Laboratorio Informatica (data, orario, classe, attività svolta) e il Registro Alunni Postazioni Computer (nome alunno associato al PC utilizzato). Non essendovi un backup automatico, i file elaborati devono essere salvati dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

3.c E-mail

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

3.d Blog e sito web della scuola

La scuola non ha un blog ma possiede un sito web. Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

3.e Protezione dei dati personali

Il personale scolastico è incaricato del trattamento dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).
Ai genitori viene fornita richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.
(Allegato n.2)

4. Strumentazione personale

Gestione degli strumenti personali - cellulari, tablet ecc..

L'uso di strumenti elettronici personali è consentito esclusivamente per scopi didattici, previa autorizzazione del docente e sotto stretta sorveglianza dello stesso.
Di seguito vengono riportate le relative norme del Regolamento d'Istituto, integrato in data 09/02/2018.

1. *E' tassativamente vietato l'uso del telefono cellulare e di altri dispositivi elettronici per motivi personali, per scopi ludici, per disturbo delle attività scolastiche e per atto di offesa verso coetanei e adulti.*
2. *All'ingresso, gli alunni hanno l'obbligo di spegnere il telefono cellulare o gli altri dispositivi elettronici e di riporli nello zaino e prelevarli ,per scopi didattici, solo se autorizzati e vigilati dai docenti.*
3. *Nel caso che l'allievo/a non ottemperi al divieto, il docente presente procederà al ritiro temporaneo del telefono cellulare e di altri dispositivi elettronici che saranno consegnati al dirigente scolastico per la necessaria custodia. Nel contempo, tale sequestro verrà annotato sul registro di classe, dandone contestuale comunicazione alla famiglia interessata, anche per riottenere l' oggetto sequestrato. Nel caso in cui nessuno dei genitori sia rintracciabile, il telefono sarà riconsegnato all'alunno al termine delle lezioni, ma egli dovrà essere accompagnato da uno dei genitori il giorno scolastico successivo, in modo che venga messo al corrente della mancanza del figlio. Integrazione del punto 4: gli alunni sono tenuti a riporre in apposito contenitore di classe il dispositivo e riprenderlo alla fine delle lezioni.*
4. *Il consiglio di classe competente, sulla base delle norme del vigente regolamento, stabilirà eventuali sanzioni disciplinari aggiuntive, rientrando il comportamento dell'allievo/a tra quelli che introducono turbativa e discontinuità nel processo educativo.*

5. Prevenzione, rilevazione e gestione dei casi

5.a Prevenzione

L'obiettivo principale della scuola è creare un ambiente di apprendimento sereno e sicuro in cui bullismo, prepotenza, aggressione e violenza non siano permessi. Gli studenti devono essere incoraggiati a parlare di sé e dei propri problemi e i loro coetanei devono saper difendere i compagni più vulnerabili, combattendo l'omertà e l'indifferenza e incoraggiando le vittime a chiedere aiuto, in modo da sottrarre al bullo potenziali proseliti.

Se è vero che la scuola ha l'obbligo di diffondere un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educhi all'accettazione, alla consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva, anche la famiglia ha un ruolo fondamentale perché nell'educare i propri figli deve saper vigilare attentamente sui loro comportamenti.

Rischi

Le principali aree di rischio per gli alunni possono essere riassunte come segue:

Contenuto

- ✓ Violenza
- ✓ Pornografia
- ✓ Razzismo / Odio

Contatto

- ✓ Molestie / Stalking
- ✓ Richieste sessuali / Grooming
- ✓ Persuasione ideologica
- ✓ Violazione della privacy / furto d'identità / abuso dei dati personali

Condotta

- ✓ Cyberbullismo
- ✓ Sexting (invio e ricezione di immagini personali intime)
- ✓ Autolesionismo, anoressia
- ✓ Divulgazione di informazioni personali

Azioni

L'istituto prevede le seguenti azioni di prevenzione:

- ✓ Informare e formare docenti, genitori, personale ATA e alunni sui rischi che un uso non sicuro delle tecnologie digitali 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 di eventuali foto, immagini, testi e disegni relativi al/la proprio/a figlio/a) (Allegato n.2)
- ✓ Non consentire l'utilizzo del cellulare personale degli alunni a scuola se non per scopi didattici previa autorizzazione del docente e sotto la sua sorveglianza
- ✓ Predisporre i PC del laboratorio d'informatica di accessi diversificati per l'alunno e per l'amministratore dotato di password, in modo che sia negata la possibilità agli studenti di scaricare e/o installare software sul dispositivo
- ✓ Utilizzare filtri e software che impediscano il collegamento a determinati siti web

Le azioni di contenimento degli incidenti previste sono le seguenti:

- ✓ Se l'alunno fa circolare immagini inappropriate in Rete, è necessario contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito, chiedere di rimuoverle.
- ✓ Se l'alunno viene infastidito od offeso suggerirgli di:
  - modificare i dettagli del proprio profilo settandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo
  - bloccare o ignorare particolari mittenti, cancellando il loro nominativo dalla lista
  - inserire la persona che offende nella cartella AntiSpam delle mail
  - cambiare il proprio indirizzo e-mail
  - scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati
  - cambiare il numero di cellulare
  - informare i propri genitori
  - cancellare il materiale offensivo dal cellulare solo dopo averlo fatto visionare

- contattare la Polizia Postale se si ritiene che il materiale offensivo sia illegale.

✓ In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò costituisce reato

5.b Rilevazione

Accorgersi di episodi di cyberbullismo non è sempre semplice perché le prevaricazioni avvengono in luoghi virtuali in cui gli adolescenti si ritrovano. E' necessario dunque cogliere i segnali che i ragazzi lanciano quando si trovano in una situazione di disagio o di difficoltà. 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, anche per fatti accaduti al di fuori della scuola. Per tale motivo è necessario confrontarsi periodicamente sui rischi delle comunicazioni on line.
Per interpretare meglio eventuali segnali è opportuno tenere presenti alcuni indicatori che ci possono aiutare per verificare se nella classe sono presenti episodi di prevaricazione. Esempi di domande stimolo utili per arrivare all'identificazione del problema sono presenti nei materiali di supporto dell'area scuole del sito generazioni connesse (Allegato n.3).

Che cosa segnalare

I contenuti "pericolosi" da segnalare sono:

✓ Contenuti afferenti la privacy: foto personali, indirizzo di casa, numero di telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà di eventi privati, credenziali d'accesso ad account personali, ecc

✓ Contenuti afferenti l'aggressività o la violenza: messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, contenuti razzisti, che inneggiano al suicidio, immagini o video imbarazzanti e/o umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.

✓ Contenuti afferenti la 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.

Questi contenuti possono essere comunicati ad altri o ricevuti da altri tramite email, possono essere pubblicati sui social network o diffusi nelle chat a causa di un utilizzo incauto, scorretto o criminoso degli strumenti digitali da parte dei minori.

Come segnalare: quali strumenti e a chi

Alunni

Per i minori non è facile avere il coraggio di denunciare episodi di cyberbullismo (grooming, sexting, ecc) o situazioni di disagio che stanno vivendo o che riguardano una persona a loro cara. I docenti sono sempre disponibili all'ascolto e al dialogo e, come già detto in precedenza, svolgono attività che affrontano le problematiche connesse ad un uso scorretto delle TIC ma, per aiutare ulteriormente i ragazzi a confidarsi, la scuola ha previsto di fornire loro alcuni strumenti specifici:

✓ il **"RobotBull"**: un robot di latta situato nell'atrio della scuola nel quale gli studenti anonimamente possono segnalare le proprie preoccupazioni o esperienze, scrivendole e imbucandole

✓ lo "**Sportello d'Ascolto**": due dottoresse in psicologia mettono le proprie competenze al servizio dei ragazzi, fornendo loro colloqui individuali (previa autorizzazione firmata dai genitori).

Docenti

I docenti devono sempre informare il referente di eventuali sospetti o di accertate evidenze e concordare tutte le conseguenti azioni da mettere in atto.

Le segnalazioni devono essere effettuate per iscritto e devono contenere tutte le informazioni necessarie alla presa in carico della situazione, pertanto, i docenti devono compilare il "Modulo segnalazione" (Allegato n.4), messo a disposizione sul sito di Generazioni Connesse.

I docenti devono provvedere a conservare le prove della condotta incauta, scorretta dell'alunno o viceversa dell'abuso subito dal minore, salvando tutte le informazioni relative, come ad esempio data, ora, contenuto dei messaggi, ID del mittente (username, mail, numero di telefono cellulare,…), indirizzo web del profilo.

Questa procedura va seguita sia per i dispositivi personali degli studenti che per quelli della scuola ma chiaramente sui primi sarà l'alunno ad effettuare il salvataggio, sui secondi il docente.

In base alla gravità dell'accaduto verranno informati il Dirigente scolastico, i genitori degli alunni e per le condotte criminose le Forze dell'Ordine.

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, anche se riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e al Dirigente scolastico; per quelle criminose, anche alla Forze dell'Ordine.

In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un 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 devono restituirla firmata per presa visione
- ✓ Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti
- ✓ Relazione scritta al Dirigente scolastico
- ✓ Convocazione scritta e colloquio con i genitori degli alunni da parte del Dirigente scolastico

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 gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

Come gestire le segnalazioni

L'Istituto adotta la procedura suggerita dal sito www.generazioni connesse.it sia per quello che riguarda la gestione delle segnalazioni sia per il loro monitoraggio costante attraverso l'utilizzo degli schemi messi a disposizione sul sito (Allegati n.5a, 5b, 6, 7, 8,).

5.c Gestione dei casi

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

Gestione dei casi di "immaturità"

Spesso tra gli studenti possono nascere interazioni animate o contrasti verbali e può esserci derisione per gioco perché viene messa alla prova la relazione tra pari, la supremazia o la parità tra i soggetti implicati e l'alternanza e la 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 possono essere controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e al rispetto degli altri, di riflessione e di confronto.

Gestione dei casi di "prepotenza" o "prevaricazione"

Gestione diversa è riservata a comportamenti e ad atteggiamenti costanti e ripetitivi di arroganza, di prepotenza, di prevaricazione, di disprezzo, di dileggio, di emarginazione, di esclusione ai danni di una o più persone, da parte di un solo soggetto o di un gruppo.
Per risolvere tali situazioni, i docenti effettuano interventi:

- ✓ sul gruppo-classe, coinvolgendo anche i genitori degli alunni, allo scopo di ristrutturare l'ambiente e le relazioni nate nel contesto della classe
- ✓ individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale
- ✓ individualizzati sui prevaricatori per far comprendere le conseguenze delle proprie azioni, per promuovere atteggiamenti empatici e per favorire una loro condivisione delle norme morali
- ✓ sul gruppo classe per favorire negli alunni un buon rapporto con il proprio corpo
- ✓ sul gruppo classe per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e nello stesso tempo far acquisire determinazione nel rifiutare i contatti anche a distanza sgradevoli o strani
- ✓ sul gruppo classe per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto.

Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito attivo presso la scuola.

Gestione di "pedopornografia"

Nel caso di contenuti, foto e video in cui minori sono coinvolti o assistono ad attività sessuali, è necessario innanzitutto evitare di eseguire 'download', produrne copie, condividerne link o postarne il contenuto in quanto ciò è reato per chiunque (la detenzione, anche temporanea, di materiale pedopornografico è illegale). Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi moduli online, disponibili sui siti www.stop-it.it e www.azzurro.it/it/clicca-e-segnala, ovvero collegandosi al sito della Polizia Postale https://www.commissariatodips.it. dove è possibile sia segnalare che denunciare. Si consiglia anche di recarsi nella sede più vicina della Polizia Giudiziaria.
Non operare in modo isolato, ma confrontarsi sempre con i colleghi di classe e il Dirigente Scolastico.

Gestione degli "abusi sessuali"

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 si riduce solo alla segnalazione, ma ovviamente è più ampio ed importante, perché ha come obiettivo principale quello di aiutare la vittima a riprendere una crescita serena. Ciò viene fatto insieme ad altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

Allegati

1. Dichiarazione genitori
2. Liberatoria genitori
3. Scheda domande/stimolo bullismo/cyberbullismo
4. Modulo segnalazione

5.a Cosa fare in caso di....bullismo (sospetto)
5.b Cosa fare in caso di....bullismo (evidenza)

6. Cosa fare in caso di....adescamento online
7. Cosa fare in caso di....sexting
8. Diario di bordo (schema riepilogo casi)

L'Animatore Digitale
Prof.ssa Ivana Scafati

Il Dirigente Scolastico
Dott.ssa Carla Farina