



MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
ISTITUTO COMPRENSIVO AD INDIRIZZO MUSICALE
DISTRETTO N. 16 Presidio di Legalità. Centro CAMBRIDGE
Macerata Campania (CE) Via Roma,11
C.F. 94017830616- Mail: ceic88300b@istruzione.it – ceic88300b@pec.istruzione.it
sito www.icmaceratacampania.gov.it Tel 0823/692435 Fax 0823/695550

E-Safety Policy

GENERAZIONI CONNESSE

-Il nostro percorso di Competenza Digitale e alla Legalità -

DIRIGENTE SCOLASTICO: PROF.SSA MASCOLO CARMELA

Referente Generazioni Connesse: Prof.ssa Trepiccione Sipontina

WEB Master: Prof. De Simone Giuseppe

E-Safety Policy

Sommario

Introduzione.....	3
1. Ruoli e Responsabilità	3
2. Condivisione e comunicazione della Policy all’intera comunità scolastica	4
3. Gestione delle infrazioni alla Policy.	4
4. Monitoraggio dell’implementazione della Policy e suo aggiornamento.	4
Integrazione della Policy con Regolamenti esistenti.	4
5. Formazione e Curricolo	5
Curricolo sulle competenze digitali per gli studenti.	5
Formazione dei docenti sull’utilizzo e l’integrazione delle TIC nella didattica.	5
Formazione dei docenti sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali	5
Sensibilizzazione delle famiglie.	5
6. Gestione dell’infrastruttura e della strumentazione ICT della scuola.	5
Accesso ad internet: filtri, antivirus e sulla navigazione.....	5
Gestione accessi.....	5
E-mail.....	6
Blog e sito web della scuola	6
Social network.	6
7. Protezione dei dati personali.	6
8. Strumentazione personale.....	6
Per gli studenti	6
Per i docenti.....	6
9. Prevenzione, rilevazione e gestione dei casi.....	6
Rischi nell’uso delle tecnologie digitali a scuola	6
Azioni di prevenzione	7
10. Le procedure interne per Rilevazione.....	7
Come gestire le segnalazioni. Gestione dei casi.....	8
11. Azioni.....	8
Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali	9

Introduzione

La realtà territoriale dell'I.C. di Macerata Campania riflette tutte le problematiche che emergono in qualsiasi comunità educativa. In particolar modo esse concernono le dinamiche relative al riconoscimento delle diversità, intese nella molteplicità delle forme che siano culturali, etniche, religiose, socio-economiche o di genere. Il passaggio dal fenomeno del "bullismo" tradizionale a quello più moderno del "Cyber bullismo", ha determinato un'accelerazione ed una diffusione su scala macroscopica tale da determinare l'intervento sinergico delle componenti interne alla comunità educante, vale a dire alunni, docenti, genitori. La creazione di una coscienza collettiva così complessa e complicata, oltre che continuamente mutevole, ha bisogno di percorsi idonei e consolidati.

Il richiamo poi, a livello nazionale, operato attraverso mezzi di informazione e WEB, oltre alle indicazioni ministeriali, vedi "**Linee di Orientamento per azioni di prevenzione e contrasto bullismo e cyber-bullismo, nota 2519, 15/4/2015**", ed infine l'istituzione della **Legge 29 maggio 2017 n. 71** recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", hanno determinato la necessità sempre crescente di un'azione mirata ed efficace da parte della scuola, consapevoli però della imprescindibile collaborazione della famiglia e degli enti territoriali.

Il presente documento, elaborato in collaborazione con il **Safer Internet Centre**, nell'ambito del progetto **Generazioni Connesse**, vuole coinvolgere tutte le componenti della Comunità scolastica: il personale della scuola, gli alunni e le famiglie per definire l'insieme di regolamenti, linee di azione e attività da porre in essere per facilitare e promuovere l'utilizzo delle TIC nella didattica e attraverso lo sviluppo di competenze digitali, determinare anche una prevenzione rispetto ai rischi delle tecnologie digitali nonché le misure di gestione di situazioni problematiche.

Si precisa che tale documento è in fase di evoluzione e per il prossimo anno è prevista la sua implementazione con un protocollo concernente la "NETIQUETTE" di Istituto redatta nel più ampio ambito del Piano Bullismo e Piano della Legalità.

1. Ruoli e Responsabilità

Le componenti della comunità scolastica, devono favorire il perseguimento degli obiettivi prefissati con ruoli diversi e obiettivi

1) Dirigente scolastico deve garantire

- Garantire una formazione adeguata del personale scolastico;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- supportare i docenti nelle procedure per la segnalazione e gestione dei casi che dovessero verificarsi.

2) Animatore digitale e il team per l'innovazione devono

- individuare i fabbisogni dell'istituto
- Cogliere monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola,
- Favorire la formazione interna per lo sviluppo della "scuola digitale" e della sicurezza in rete
- proporre soluzioni metodologiche e tecnologiche innovative e sostenibili

3) Docenti

- Formarsi sull'utilizzo delle tecnologie digitali, sulle problematiche attinenti
- Applicare il regolamento
- Garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche
- Garantire l'applicazione del **REGOLAMENTO SULL'USO DI DISPOSITIVI ELETTRONICI DA PARTE DEGLI ALUNNI** approvato dal Collegio dei Docenti
- Favorire un uso critico e consapevole di Internet a scuola e a casa,
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;

4) Alunni:

tenendo conto del grado di maturità e di apprendimento, devono

- rispettare REGOLAMENTO SULL'USO DI DISPOSITIVI ELETTRONICI DA PARTE DEGLI ALUNNI
- costruire una cittadinanza digitale comprendendo le potenzialità offerte dalle TIC
- conoscere e rispettare il diritto d'autore
- conoscere le buone pratiche di sicurezza on-line
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- comunicare con gli adulti di riferimento sull'uso e sui rischi delle tecnologie e della rete

5) Genitori

- Collaborano con la comunità scolastica per l'utilizzo consapevole delle TIC nella didattica;
- Contrattano le regole per un utilizzo corretto delle TIC e della rete
- Monitorano l'uso che i figli fanno di internet e dei vari dispositivi.

2. Condivisione e comunicazione della Policy all'intera comunità scolastica

Il presente documento verrà pubblicizzato in seno al Consiglio di Istituto, Collegio Docenti, Consigli di Classe e messo all'albo istituzionale, alla voce concernente Osservatorio "IO S...BULLO" gestito nell'ambito del Piano Bullismo dalla Referente al Bullismo di Istituto e dal Web Master.

Sono previsti inoltre:

- Incontri-riflessioni con figure professionali di riferimento
- Incontri formativi con genitori
- Incontro con POLIZIA POSTALE
- Incontro con arma dei CARABINIERI
- Safer Internet Day 2019
- Attività collegate a "GENERAZIONI CONNESSE"
- Attività collegate a "SCUOLA AMICA"
- Attività e collaborazione/interscambio con tutto ciò che concerne EDUCAZIONE ALLA LEGALITÀ
- Convegno genitori gestito da alunni

3. Gestione delle infrazioni alla Policy.

La violazione delle norme previste dal REGOLAMENTO SULL'USO DI DISPOSITIVI ELETTRONICI DA PARTE DEGLI ALUNNI comporta l'eventuale irrogazione di sanzioni disciplinari, secondo quanto previsto dal Regolamento di disciplina e dal Patto di Corresponsabilità controfirmato da scuola e genitori all'atto dell'iscrizione. Nei casi più gravi potrebbero anche configurarsi reati perseguibili d'ufficio o a querela di parte, come previsto dai riferimenti normativi e da specifica norma n.71 del 29 maggio 2017.

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

Il monitoraggio dell'implementazione della policy e il suo eventuale aggiornamento sarà svolto annualmente dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale, del Team per l'innovazione e dal Referente Bullismo.

Integrazione della Policy con Regolamenti esistenti.

La Policy va ad integrarsi con gli obiettivi del PTOF, con il Regolamento di Istituto, con il Regolamento sull'uso dei dispositivi elettronici e con la normativa vigente.

5. Formazione e Curricolo

Curricolo sulle competenze digitali per gli studenti.

“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 implica abilità di base nelle tecnologie dell’informazione e della comunicazione (TIC): l’uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.” Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali 2012. Pertanto tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

Non a caso tale competenza viene individuata come una Competenza Chiave declinata come segue: “Utilizzare e produrre strumenti di comunicazione visiva e multimediale, anche con riferimento alle strategie espressive e agli strumenti tecnici della comunicazione in rete. Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare”.

All’interno del PNSD l’Istituto Comprensivo di Macerata Campania porta avanti azioni volte ad innovare la didattica tradizionale avvalendosi di “Google classroom”, “Piattaforma Open Class”, “L’ora del Codice”, “Moduli di google drive”, “Classe 2.0”.

Formazione dei docenti sull’utilizzo e l’integrazione delle TIC nella didattica.

Ogni anno si procede con l’aggiornamento per la formazione sul digitale gestita dall’A.D. nell’ambito del PNSD.

Formazione dei docenti sull’utilizzo consapevole e sicuro di Internet e delle tecnologie di gitali

Con la partecipazione dell’Istituto al progetto “Generazioni Connesse” del Safer Internet Center. Si prevede anche una fase di autoaggiornamento degli insegnanti tramite materiali informativi sulla sicurezza in internet reperibili sul web, in particolare sul sito di Generazioni Connesse (www.generazioniconnesse.it). E’ presente il Referente per il bullismo e cyberbullismo.

Sensibilizzazione delle famiglie.

Nell’ambito del progetto “Generazioni Connesse”, alla relativa pagina Osservatorio “IO S...BULLO”, del sito www.icmaceratacampania.gov.it, sono pubblicizzati i materiali a disposizione delle famiglie per sensibilizzarle sui problemi legati ad un uso non corretto di internet e delle tecnologie digitali, anche al di fuori della scuola, ivi incluso Piano Bullismo e Progetto relativo.

6. Gestione dell’infrastruttura e della strumentazione ICT della scuola.

Accesso ad internet: filtri, antivirus e sulla navigazione.

L’accesso a internet è possibile e consentito per la didattica in tutti i plessi della primaria e della secondaria di primo grado, attraverso reti LAN e WiFi; al momento l’accesso per gli studenti non risulta filtrato quindi le credenziali delle WiFi non devono essere loro fornite, e il lavoro sulle postazioni fisse è vigilato e mediato dai docenti.

Gestione accessi

(password, backup, ecc.). L’accesso alla rete è comune per ogni plesso e permette tramite rete LAN o Wifi (attraverso l’impostazione di una password) di accedere al web per esigenze didattiche e per redigere giornalmente il registro elettronico.

E-mail.

Ogni plesso è dotato di un account di posta elettronica che sarà utilizzato ordinariamente dagli uffici per l'invio della documentazione di servizio. La posta elettronica istituzionale gestita dalla segreteria è protetta da antivirus, e quella certificata anche dall'antispam.

Blog e sito web della scuola

La scuola attualmente ha un sito web aggiornato, www.icmaceratacampania.gov.it, in cui sono pubblicati i contenuti delle proposte formative e del settore didattico, nonché le circolari e quanto previsto dal CAD. Inoltre sono attivi due Blog: "IO S...BULLO", Blog alunni, Blog "Voce agli studenti".

Social network.

Attualmente i Docenti stanno sperimentando l'uso di piattaforme didattiche protette: social learning interamente dedicati alla didattica per creare classi virtuali, condividere risorse, realizzare contenuti multimediali, assegnare verifiche e dialogare in maniera "social" tra docenti, studenti e famiglie

7. 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). Tutto il personale incaricato riceve poi istruzioni particolareggiate, applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. All'inizio dell'anno scolastico, viene inoltre fornita ai genitori

- informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

- liberatorie per l'utilizzo delle immagini

- responsabile trattamento dati personali

il tutto consultabile su homepage istituzionale

8. Strumentazione personale

Per gli studenti

La gestione degli strumenti personali - cellulari, tablet ecc.. è normata dal REGOLAMENTO SULL'USO DI DISPOSITIVI ELETTRONICI DA PARTE DEGLI ALUNNI

Per i docenti

Durante le lezioni è consentito l'utilizzo di smartphone, tablet, ecc. solo a scopo didattico, ad integrazione degli strumenti scolastici disponibili

9. Prevenzione, rilevazione e gestione dei casi

Rischi nell'uso delle tecnologie digitali a scuola

Si possono verificare due situazioni

- 1) uso improprio degli strumenti personali, per scopi non didattici, anche in spazi diversi dall'aula, acquisire e pubblicare in rete. foto o video propri o di altri, anche a contenuto improprio
 - pubblicare messaggi o commenti lesivi della dignità o della reputazione altrui
 - accedere a contenuti e siti non adatti ai minori
 - ascoltare musica, utilizzare giochi, chat, ecc.
 - entrare in contatto con sconosciuti

2) navigazione in internet mediante gli strumenti presenti a scuola.

- Accedere a contenuti inappropriati
- infettare i computer o i tablet con virus o malware scaricando materiali, installando programmi e applicazioni, utilizzando dispositivi personali di memoria come pennette USB
- utilizzare materiale illegale, violare il diritto d'autore o di proprietà.

Azioni di prevenzione

Si prevede l'implementazione e il miglioramento della navigazione in INTERNET tramite:

- installazione di filtri sul server e sul motore di Ricerca
- il blocco di finestre pop up,
- verifica della cronologia.
- Utilizzo di cloud

Educare la comunità scolastica a:

- un uso consapevole e responsabile della rete
- proteggere la propria identità,
- creare password efficaci
- riflettere sulle possibili conseguenze prima di postare foto o video propri e non postare foto e video di altri senza il loro consenso
- rispettare il copyright, e citare le fonti

Prevenire (anche con l'intervento di specialisti)

- Insegnare a riconoscere e a confidarsi con adulti di riferimento rispetto a situazioni di rischio
- Conoscere I servizi messi a disposizione dal Safer Internet Center per segnalazioni, anche anonime, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete: "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children e della linea di ascolto 1.96.96 di Telefono Azzurro legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

10. Le procedure interne per Rilevazione

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

Che cosa segnalare

Qualora si riscontri la pubblicazione di:

- _ dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);
- _ contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- _ contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc. andranno opportunamente segnalati per gli interventi opportuni.

Come segnalare: quali strumenti e a chi.

Il personale della scuola, anche con l'ausilio tecnico dell'Animatore Digitale, provvederà a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola nonché la data e l'ora. Nel caso di messaggi, si cercherà risalire al mittente attraverso i dati del suo profilo. Si cercherà di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, alla famiglia ed, eventualmente, alla Polizia Postale .

Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto.

In base alla gravità dei fatti si provvederà:

- a una comunicazione scritta tramite diario alle famiglie;
- a una nota disciplinare sul registro on-line;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente scolastico;

per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

Come gestire le segnalazioni. Gestione dei casi

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

La gestione dei casi rilevati va differenziata a seconda della loro gravità; è opportuno condividere ogni episodio con il team docenti. Alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. In altri è opportuno convocare genitori e alunni per cercare di rimediare all'accaduto. Nei casi più gravi occorre sottoporre all'attenzione del Dirigente Scolastico l'accaduto perché predisponga le azioni da intraprendere.

- _ E' opportuno promuovere campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni.
- _ Portare a conoscenza degli alunni che per la legge italiana il cyber-bullismo, la diffusione e il possesso di materiale pornografico è reato e che una foto o un video diffuso in rete potrebbero non essere tolti mai più.
- _ Sensibilizzare la popolazione studentesca sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.
- _ Coinvolgere i genitori per attivare forme di controllo della navigazione e monitorare l'esperienza online dei propri figli.
- _ Tutelare la privacy e informare sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farli rispettare.
- _ I docenti, in classe, parlano di bullismo, adescamento, uso sicuro di internet e dei social network, sexting, cyberbullismo e delle conseguenze. Propongono riflessioni sulle menzogne dette per stringere relazioni online.
- _ Promuovere la consapevolezza e le conoscenze sul cyberbullismo, attraverso corsi di formazione, seminari, dibattiti. E' infatti importante che docenti, personale ATA, genitori e studenti abbiano una chiara e condivisa definizione di cyberbullismo. Informare i docenti, il personale ATA ed i genitori sui comportamenti non verbali correlati al cyberbullismo. Gli adulti dovrebbero allertarsi se uno studente, dopo l'uso di internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura. Aggiornare il Regolamento di Istituto prevedendo apposite norme in tema di cyberbullismo e navigazione on line sicura. Specificare quando e come si possono utilizzare all'interno della scuola, i computers ed i videotelefonini.
- _ Segnalare agli alunni l'esistenza di una linea di ascolto 19696 attiva tutto l'anno 24 ore su 24 di telefono azzurro che raccoglie richieste di ascolto e di aiuto. Al servizio HOTLINE si possono segnalare, in forma anonima, contenuti pedopornografici e altri contenuti dannosi diffusi dalla rete. Sono a disposizione dei servizi quali: Telefono Azzurro, Save the Children, Polizia Postale.
Per tutti i casi che costituiscono reato occorre informare il Dirigente Scolastico per confrontarsi sulle azioni da intraprendere ed eventualmente attivare l'intervento delle forze dell'ordine.
Non esistono protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi, tuttavia si praticano forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo con gli Enti Locali e il Comando dei Carabinieri.

11.AZIONI

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati. Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

- _ diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- _ richiedere all'inizio di ogni anno scolastico autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);
- _ far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;

Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali sono:

- _ bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- _ controllare periodicamente i siti visitati dagli alunni;
- _ affidare a un gruppo di docenti scelto le regole di filtraggio.

Per tutti gli allegati consultare il sito Istituzionale.

Referente Generazioni Connesse
Prof.ssa Sipontina Trepiccione

F.to IL DIRIGENTE SCOLASTICO
(Prof.ssa Carmela Mascolo)
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2, del D. L.vo 39/1993