ISTITUTO COMPRENSIVO DI MELDOLA
Viale della Repubblica, 47 – 47014 MELDOLA (FC)
Tel. 0543/496420-495177 – Fax 0543/490305 –
e-mail: foic81100c@istruzione.it - foic81100c@pec.istruzione.it
Sito web **www.icsmeldola.gov.it**

POLICY DI E-SAFETY

Approvato dal Collegio Docenti in data 18/06/2018
e dal Consiglio di Istituto in data 28/06/2018

E-Safety Policy

INDICE

1 INTRODUZIONE

"La progettualità relativa alla tutela della sicurezza informatica in generale, e del contrasto al cyberbullismo, in particolare, deve operare su due livelli paralleli: la conoscenza dei contenuti tecnologici e la conoscenza delle problematiche psico-pedagogiche correlate.

E' fondamentale, perciò, far comprendere la nozione basilare secondo cui la propria ed altrui sicurezza in Rete non dipende solo dalla tecnologia adottata (software, anti-virus, anti-malware etc.) ma dalla capacità di discernimento delle singole persone nel proprio relazionarsi attraverso la Rete.

Azioni mirate alla sicurezza nella Rete sono, dunque, necessarie per affrontare tali problematiche: non vanno, infatti, colpevolizzati gli strumenti e le tecnologie e non va fatta opera repressiva di quest'ultime; occorre viceversa, fare opera d'informazione, divulgazione e conoscenza per garantire comportamenti corretti in Rete, intesa quest'ultima come "ambiente di vita" che può dar forma ad esperienze cognitive, affettive e socio-relazionali."

Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo 2015

PREVENIRE E CONTRASTARE
fenomeni di
BULLISMO e CYBERBULLISMO
vuol dire
EDUCARE ALLA RELAZIONE

La Scuola, in quanto Comunità educante, ha il dovere di mettere in campo azioni mirate allo sviluppo delle *social skills*: empatia, rispetto, senso critico e assertività, ossia esprimere le proprie emozioni e opinioni senza ledere i diritti altrui.
Far lavorare bambini e ragazzi a coppie o in piccoli gruppi in modo sistematico e continuativo sullo sviluppo delle social skills è un modo agevole e divertente di educare gli studenti alla Relazione.

1.1 Scopo della Policy

Scopo del presente documento è di informare l'intera comunità scolastica sull'uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione all'Istituto, nel pieno rispetto della normativa vigente.
In particolare, l'intento è quello di:

- promuovere l'uso consapevole e critico da parte delle alunne e degli alunni delle tecnologie digitali e di Internet;
- far acquisire competenze digitali e corrette norme comportamentali;
- prevenire, rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso delle tecnologie dell'informazione e della comunicazione
- curare e sostenere il percorso di crescita emotiva e relazionale degli alunni e delle alunne nel processo di maturazione della loro identità e della loro autonomia.

1.2 Riferimenti normativi

- LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e al cyber bullismo – nota MIUR n. 2519 aprile 2015;

- Indicazioni operative per l'attuazione delle LINEE DI ORIENTAMENTO per azioni di contrasto al bullismo e al cyber bullismo – Nuovi ruoli e compiti assegnati ai CTS nota USR n. 16367/2015

- Piano nazionale per la prevenzione del Bullismo e del Cyberbullismo a scuola a.s. 2016/2017 – nota MIUR n. 11419/2016

- Legge n. 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo;

- Aggiornamento LINEE DI ORIENTAMENTO per la prevenzione e il contrasto del cyber bullismo – nota MIUR n. 5515 ottobre 2017.

1.3 Ruoli e responsabilità

RUOLO	RESPONSABILITA'
DIRIGENTE SCOLASTICO	-Responsabilità generale per la sicurezza dei dati; -garantire l'uso di un Internet Service conforme alle normative vigenti; - prouovere il documento e safety policy -ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; -assicurare che l'educazione alla sicurezza online sia incorporata all' interno del PTOF; -assicurare che tutto il personale sia a conoscenza delle procedure da seguire in caso di incidente per la sicurezza online.
RESPONSABILE DELLA SICUREZZA ONLINE (DSGA E DOCENTI SU NOMINA DS)	-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 (circolari, sito web, ecc) all' interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente Scolastico e dell' animatore Digitale nell' ambito dell'utilizzo delle tecnologie digitali e di Internet.
ANIMATORE DIGITALE E SUO TEAM	-Stimolare la formazione interna all'Istituzione

	negli ambiti di sviluppo della "Scuola digitale"e fornire consulenza e informazioni al personale sui rischi online e sulle misure di prevenzione e gestione degli stessi; -assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate; -curare la manutenzione del sito web della scuola per scopi istituzionali e consentiti; -coinvolgere la comunità scolastica (alunni, genitori….) nella partecipazione alle attività e ai progetti attinenti le TIC.
INSEGNANTI	-Inserire temi legati alla sicurezza online nella programmazione di classe; -informarsi e aggiornarsi sulle problematiche attinenti la sicurezza nell' utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola. -rispettare il regolamento e-policy dell'Istituto; -favorire l' utilizzo corretto e sicuro delle TIC e di Internet accertandosi che siano integrate nel curriculum di studio e nelle attività didattiche e educative delle classi; -favorire la comprensione e il rispetto delle regole per prevenire e contrastare l' utilizzo scorretto e pericoloso delle TIC e di Internet; -assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte delle 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 dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali. -assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente.
PERSONALE SCOLASTICO	-Comprendere e contribuire a promuovere politiche di e-Security; -essere consapevoli dei problemi di sicurezza online connessi con l' uso di telefoni cellulari, fotocamere e dispositivi portatili; -monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche riguardo gli stessi; -segnalare qualsiasi abuso, sospetto o problema ai responsabili dell' e-Security; -tenere comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; -garantire che le comunicazioni digitali con gli

	studenti siano di tipo professionale e avvengano solo attraverso i sistemi scolastici previsti.
ALUNNI	-Leggere ,comprendere accettare e applicare l' e-Safety Policy attraverso la mediazione dei docenti in relazione all'età. -essere responsabili riguardo al proprio grado di maturità e di apprendimento, per l' 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. Evitare il plagio e rispettare i diritti d' autore; -comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi; -adottare condotte rispettose degli altri anche quando si comunica in rete; -chiedere chiarimenti nell' utilizzo delle tecnologie didattiche e/o di Internet a docenti e genitori; -capire l'importanza di segnalare abusi, l'uso improprio dei dispositivi tecnologici o l' accesso a materiali inappropriati.
GENITORI	-Sostenere la linea di condotta della scuola adottata nei confronti dell' utilizzo delle tecnologie dell' Informazione e delle Comunicazioni nella didattica; -seguire gli alunni 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 di Internet e del telefonino; -concordare con i docenti, su loro proposta, linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet; -fissare delle regole per l' utilizzo del computer e del telefonino; -tenere sotto controllo e monitorare l' uso che i figli fanno di Internet e del telefonino in generale.

1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica

Le linee guida per l'e-Safety Policy intendono disseminare all'interno del nostro Istituto una maggiore "cultura dell'uso corretto e consapevole di Internet", sia tramite il richiamo a norme vigenti, sia tramite l'indicazione di prassi adeguate all'uso sempre più professionale di Internet da

parte di tutto il personale. Si vuole, inoltre, educare l'intera comunità scolastica alla prevenzione dei rischi e alla gestione delle emergenze legati a questo strumento.
Le linee guida fanno riferimento a un uso generale delle infrastrutture di rete e costituiscono una parte integrante del Regolamento di Istituto. Sono portate a conoscenza degli Organi Collegiali e di tutti gli operatori e gli utenti della scuola: con questo documento si intende attivare e mantenere nel nostro Istituto un'e-Safety Policy in materia di tecnologie dell'informazione e della comunicazione condivisa e accettata da tutti.

La rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati dagli alunni solo con l'autorizzazione dei docenti stessi. L'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla rete. Sarà data particolare attenzione all'educazione sulla sicurezza agli aspetti per i quali gli alunni sono più esposti o rispetto ai quali sono più vulnerabili.

1.5 Gestione delle infrazioni alla Policy

1.5.1 Disciplina degli alunni

Le potenziali infrazioni in cui gli alunni possono incorrere a scuola nell'utilizzo delle tecnologie sono le seguenti:

* un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
* l'invio imprudente o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
* la condivisione d'immagini intime e/o troppo spinte;
* la comunicazione avventata e senza permesso con sconosciuti;
* il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento come previsto dal nostro Regolamento di disciplina.

Secondo le necessità, possono essere previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di sviluppo di rapporti d'amicizia, di sviluppo della conoscenza e della gestione delle emozioni.

1.5.2 Disciplina del personale scolastico

Le potenziali infrazioni, indicate in seguito, in cui il personale scolastico e i docenti incorrono nell' utilizzo delle tecnologie e di Internet possono determinare, favorire o avere conseguenze sull' uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività d' insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un' adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una parziale istruzione preventiva degli alunni sull' uso corretto e responsabile delle tecnologie digitali e di Internet;
- una vigilanza elusa degli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- nelle situazioni critiche di contrasto a terzi, insufficienti interventi correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente Scolastico, all' Animatore Digitale e al Referente per il cyberbullismo.

Il Dirigente Scolastico può controllare l' utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l' accesso a Internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni di casi di violazione del regolamento come su indicato e per l' avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, secondo il tipo o la gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

1.5.3 Disciplina dei genitori

Alcune condizioni e condotte dei genitori possono favorire o no l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori dell'ambiente scolastico.

Le situazioni familiari meno favorevoli sono:

- la convinzione che, se il proprio figlio rimane a casa a usare il computer, è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare e dello smartphone;
- un utilizzo del PC in comune con gli adulti che possono conservare in memoria materiali non idonei o dati riservati.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse.

1.6 Monitoraggio dell'implementazione della Policy e suo aggiornamento

L'eventuale aggiornamento della Policy sarà finalizzato ad una migliore aderenza alle situazioni che si presentano nell'Istituto affinchè le azioni di prevenzione, gestione e contrasto siano efficaci.

L'aggiornamento della Policy sarà curato dal Dirigente Scolastico, dall'Animatore Digitale, dal Referente per il cyberbullismo e dagli Organi Collegiali, secondo gli aspetti considerati.

2 FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

La competenza digitale è ritenuta dall'Unione Europea una competenza chiave per la sua importanza e pervasività nella società attuale. Le Indicazioni Nazionali non consentono, però, di definirla con gli stessi modi con cui si possono declinare le competenze chiave delle discipline, nonostante si ritrovino abilità e conoscenze che prevedono una competenza digitale in tutte le materie di studio. Competenza digitale implica padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie con "autonomia e responsabilità", nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

L'Istituto si impegnerà ad elaborare un curricolo sulle competenze digitali per l'anno scolastico 2018/2019.

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

Le azioni formative realizzate dall'Animatore Digitale e dal team hanno innescato un circolo virtuoso che ha stimolato sempre più docenti a utilizzare e integrare le TIC nella didattica.

Il corpo docente ha partecipato a corsi di formazione anche nell'ambito del PNSD (Piano Nazionale Scuola Digitale), oltre che a iniziative organizzate dall'istituzione raggiungendo una buona base di competenze. Particolare rilevanza ha assunto l'avvio della sperimentazione della piattaforma *G-Suite For Education* nella scuola secondaria di I grado.

L'utilizzo della piattaforma consente agli alunni di frequentare ambienti virtuali sicuri e controllati.

Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non si esaurisce nell'arco di un anno scolastico e può pertanto prevedere momenti di autoaggiornamento, di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore Digitale.

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle Tecnologie Digitali

Oltre alla partecipazione progetto "Generazioni connesse" per alunni, genitori e docenti, alcuni insegnanti della scuola hanno partecipato a incontri formativi interni all'Istituto.

- Nel corso del triennio 2014/2015/2016 l'Istituto ha organizzato momenti di informazione/formazione rivolta agli alunni e alle famiglie, con l'intervento della Polizia Postale di Forlì e del Comando dei Carabinieri della Stazione di Meldola.
- Nell'anno scolastico 2014/2015 l'Istituto ha organizzato una formazione interna, rivolta al personale docente e alle famiglie, sull'uso consapevole e responsabile delle nuove tecnologie. Relatore: Dott. Rasponi Francesco.

- Nell'anno scolastico 2015/2016 l'Istituto ha partecipato ai Progetti ***#OFF4Aday*** e **Per un WEB sicuro** promossi dall'associazione MOIGE.
- Nell'anno scolastico 2016/2017 l'Istituto ha partecipato al Progetto ***Generazioni Connesse*** (SIC ITALY III). E' stata organizzata una giornata di formazione rivolta agli alunni della scuola secondaria di I grado e alle famiglie dell'Istituto. Relatore: Dott. Giovanni Salerno – Associazione Telefono Azzurro.
- Nel corrente anno scolastico 2017/2018 l'Istituto ha organizzato un'Unità Formativa di ambito territoriale, rivolta ai docenti di scuola primaria e di scuola secondaria di I grado dell'ambito di Forlì, dal titolo "*Coesione sociale e prevenzione del disagio giovanile globale: azioni di prevenzione e di contrasto al bullismo e al cyberbullismo*". Relatore: Dott. Bilotto Andrea.

3 GESTIONE DELLA STRUMENTAZIONE TECNOLOGICA DELL'ISTITUTO

3.1 Regole generali

L'Istituto si impegna ad attuare tutte le azioni necessarie per garantire agli studenti l'accesso a siti didattici o a materiale da cercare, adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione.

Purtroppo non è sempre possibile garantire una navigazione totalmente priva di rischi e l'Istituto e gli insegnanti non possono assumersi le responsabilità derivanti da un accesso accidentale e/o improprio a siti illeciti. Al fine di ridurre i rischi si dispone quanto segue:
durante l'attività didattica l'uso del cellulare o di altri dispositivi elettronici da parte degli studenti è consentito solo come strumento didattico, mentre rappresenta un elemento di distrazione degli stessi e dei compagni ed anche una grave mancanza di rispetto nei confronti del docente se usato a scopo personale.
Pertanto:

1. E' fatto divieto a tutti gli studenti di utilizzare o comunque tenere accesi il telefono cellulare e altri dispositivi elettronici (fotocamere, videocamere…) di loro proprietà o in loro possesso senza l'autorizzazione del docente durante l'attività didattica , ai sensi dell'art.3 del D:P.R. 249/98 (Statuto delle studentesse e degli studenti).

2. E' fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo per scopi puramente didattici.

3. E' altresì fatto divieto ai docenti, ai sensi della C.M. 362/98 di utilizzare telefoni cellulari, per uso personale, durante lo svolgimento delle attività di insegnamento.

4. Nel caso in cui un docente o un collaboratore scolastico accertino l'utilizzo o comunque il funzionamento di telefono cellulare o di altro apparecchio di cui sopra da parte di uno studente in modo difforme da quanto in precedenza stabilito, sarà immediatamente applicato quanto previsto dal nostro Regolamento di Disciplina

5. Ai sensi e per gli effetti della normativa vigente, quando la violazione disciplinare può configurare un'ipotesi di reato, il Dirigente Scolastico è tenuto alla presentazione di denuncia alle autorità competenti.

Per i provvedimenti disciplinari si fa riferimento al Regolamento di disciplina riportato nel PTOF di Istituto.

3.2 Regolamento per l'utilizzo del laboratorio di informatica, dell'Aula 3.0 e dell'Atélier creativo

L'utilizzo delle attrezzature deve essere legato esclusivamente a scopi didattici. Gli studenti della scuola potranno accedere al locale solo se accompagnati da un docente. L' utilizzo del PC e delle attrezzature comporta l'accettazione incondizionata del presente regolamento.
Per la prevenzione degli incendi e il piano di evacuazione si fa riferimento alle disposizioni valide per l'intero Istituto.
Il Laboratorio è dotato di registro per organizzazione oraria delle classi.

3.3 Norme generali di comportamento

Le regole fondamentali per un corretto utilizzo del laboratorio sono le seguenti:

1. Il laboratorio è a disposizione di tutte le classi dal lunedì al sabato.
2. Ogni insegnante è tenuto ad aprire e chiudere l'aula mediante richiesta e riconsegna delle chiavi ai collaboratori scolastici. Non è consentita la consegna delle chiavi agli alunni.
3. Il docente ha il compito di compilare dettagliatamente e in ogni parte un apposito registro posto all'interno dell'aula informatica.
4. Sul registro devono essere annotati la classe, l'insegnante accompagnatore e le eventuali problematiche riscontrate (ad es. PC mal funzionanti).
5. Ogni insegnante è tenuto a procedere all'accensione del computer e all'iniziale verifica dell'integrità dei sistemi.
6. In laboratorio non è consentito consumare alcuna tipologia di pasto. Nel caso dovesse coincidere con il momento della ricreazione,gli alunni sono obbligati a uscire dall'aula computer, consumare la loro merenda e rientrare a ricreazione ultimata.
7. All'uscita è cura del docente e degli alunni risistemare tastiere, mouse, sedie quant'altro come sono stati trovati all'ingresso.
8. Gli alunni sono tenuti a rispettare le consegne dell'insegnante sull'utilizzo dei PC.
9. Gli alunni non dovranno mai essere lasciati a operare da soli, senza la supervisione del docente accompagnatore.
10. È vietato modificare in alcun modo l'hardware e il software di sistema.
11. Non modificare né inserire password di sistema.
12. Non modificare le configurazioni del sistema operativo del PC (sfondi, colore…).
13. Inserire i propri file in cartelle personali avendo cura di non cancellare documenti elaborati da altri utenti.
14. L'utente è tenuto a rispettare le regole imposte dall'uso della rete e di Internet.
15. Gli utenti sono tenuti a garantire il corretto utilizzo delle apparecchiature e a usarle in modo da evitare qualsiasi danneggiamento hardware e software. In casi particolarmente gravi

potranno essere ritenuti responsabili di eventuali danneggiamenti delle attrezzature.

16. Ogni circostanza, situazione anomala, irregolarità rispetto al presente regolamento e malfunzionamento dell'attrezzatura, in particolare la presenza di software illegale e/o di contenuti non idonei, deve essere segnalata tempestivamente al responsabile del laboratorio o al DSGA.
17. È severamente vietato staccare cavi elettrici da ciabatte e prese, così come i cavi di connessione alle periferiche.

3.4 Uso di internet

1. La ricerca su internet e l'uso della posta elettronica sono destinate alle sole finalità didattiche, scientifiche e di ricerca.
2. Tutte le macchine presenti in laboratorio sono dotate di accesso a Internet.
3. Username e password di accesso a Internet sono assegnate solo al personale docente; gli alunni possono navigare su Internet solo se sorvegliati direttamente dal docente, il quale è tenuto a verificare continuamente la navigazione degli stessi ed è direttamente responsabile dell'utilizzo di Internet da parte degli alunni cui ha dato la possibilità di collegarsi alla rete.
4. I docenti accompagnatori hanno il compito di controllare i materiali scaricati dagli alunni durante la navigazione.

3.5 Utilizzo delle stampanti

1. La stampa di documenti da parte degli alunni deve avvenire dietro esplicita autorizzazione del docente.
2. Non è consentita, né ad alunni né ai docenti, la stampa di un numero elevato di pagine, o di lavori che prevedano un consumo particolarmente oneroso d'inchiostro e carta.

TUTTI I DOCENTI che, a qualsiasi titolo, utilizzano il laboratorio sono pregati di:

1. Leggere questo regolamento agli studenti, all'inizio di ogni anno scolastico, spiegando i motivi che stanno alla base delle regole in esso contenute.
2. Rispettare rigorosamente l'orario di accesso e uscita dai laboratori.
3. Vigilare affinché durante l'ora di lezione in laboratorio sia rispettato da parte di tutti gli utenti il "Regolamento laboratorio d'informatica, dell'Aula 3.0, dell'Atélier creativo".
4. Ricordare a tutti gli alunni che nel caso fosse rilevato un danno o comunque un malfunzionamento, si riterranno responsabile coloro che hanno utilizzato il laboratorio in orario precedente alla rilevazione del problema; costoro saranno tenuti al risarcimento relativo.
5. Fare in modo che le classi non siano lasciate a lavorare senza sorveglianza.

3.6 Principali norme per gli insegnanti e per gli studenti sull'utilizzo della Piattaforma di Istituto *G suite for education*

3.6.1 Principali norme per gli insegnanti

1. Ogni insegnante è garante nei confronti del Dirigente Scolastico dell'utilizzo della piattaforma in base alle disposizioni presenti in questo documento e più in generale al codice disciplinare e al codice di condotta.

2. Durante le attività a scuola che prevedono l'utilizzo della piattaforma l'insegnante deve vigilare sugli alunni.
3. L'invio di tutte le comunicazioni è regolato esclusivamente dagli insegnanti.
4. In piattaforma possono essere usati solo i nomi propri degli studenti.
5. Eventuali foto degli studenti non devono essere corredate dai nomi e non devono contenere primi piani degli stessi nel caso in cui non sia stata concessa la liberatoria.
6. Agli studenti non sono forniti indirizzi di posta elettronica dal docente.
7. L'insegnante deve ispezionare periodicamente i settori di competenza della piattaforma per controllare l'eventuale interazione tra gli studenti e l'utilizzo corretto delle parti comuni.
8. L'insegnante deve controllare che le fonti siano sempre citate dagli alunni. Di norma occorre il permesso per riprodurre materiali quali testi, suoni, immagini o video clip. Per questo è importante controllare sempre le leggi sul copyright.

3.6.2 Norme per lo studente

1. L'accesso alla piattaforma può avvenire sia da scuola, sia da casa, se disponi della connessione Internet e di un computer.
2. Per il login utilizza solo la tua password e il tuo username.
3. Se accedi a informazioni di un altro account, non utilizzarle mai.

Norme per la salvaguardia della tua privacy e della tua sicurezza

1. Non comunicare mai il tuo username la tua password a compagni o ad altre persone.
2. L'inoltro di tutte le comunicazioni della classe è regolato e controllato esclusivamente dai tuoi insegnanti.
3. Non comunicare con altri utenti di internet senza il permesso e la presenza degli insegnanti.
4. Ti è permesso solo l'accesso ai collegamenti consentiti. L'uso dei motori di ricerca è consentito solo quando è presente un insegnante o un altro adulto.
5. Nel tuo spazio di lavoro puoi accedere solo tu, i tuoi professori e gli amministratori della piattaforma,questi ultimi per gestirla da un punto di vista tecnico.

Norme per la salvaguardia del diritto d'autore (copyright)

Normalmente occorre il permesso per riprodurre materiali quali test, suoni, immagini o video clip. In molti casi questo è possibile e molti autori darebbero volentieri il permesso. Basta chiedere e citare la fonte. In alternativa puoi fare riferimento a materiale non coperto da copyright (vedi siti dedicati). Se ciò non è possibile devi comunque citare sempre la fonte dei materiali che (testi, immagini, video clip e suoni) nei tuoi elaborati. Ad esempio se riporti un brano di testo scritto da un'altra persona, questo deve iniziare e concludersi con le virgolette "…"; al termine devi scrivere il nome ed il cognome dell'autore, il titolo della pubblicazione, la casa editrice e l'anno di pubblicazione - es. Luigi Rossi, Storia d'Italia, Bianchi Editore, 2010-oppure l'indirizzo del sito – es.www.rinascita-livi.it-.)

3.7 La Netiquette

La netiquette, è un insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi che la rete offre, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newgroup, mailing list, forum, blog o email.
In particolar modo devi rispettare le seguenti regole:

1. Se mandi un messaggio al tuo professore attraverso il forum è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema.
2. Non scrivere in maiuscolo tutto il messaggio, perché ciò vorrebbe dire urlare nei confronti dell'interlocutore, cioè del destinatario del tuo messaggio.
3. Non divagare rispetto all'argomento del forum.
4. Non condurre "guerre di opinione" nel forum a colpi di messaggi e contro-messaggi.
5. Non essere intollerante con chi commette errori sintattici o grammaticali. Chi scrive è comunque tenuto a migliorare il proprio linguaggio in modo da essere comprensibile alla collettività.
6. Rispetta le persone diverse per nazionalità, cultura, religione, sesso: il razzismo ed ogni tipo di discriminazione razziale non sono ammessi.
7. Non fornire informazioni errate, imprecise, incomplete,ambigue e in caso di dubbio,verifica prima.
8. Non rivelare dettagli ed informazioni o informazioni personali o di altre persone (indirizzi numeri di telefono).
9. L'invio e la ricezione di allegati alle e-mail devono eventualmente essere concordati con i genitori.

10. Richiedi sempre il permesso prima di iscriverti a qualche concorso, mailing-list o sito web che lo richieda.
11. Non dare indirizzo e numero di telefono a persone incontrate sul web, senza chiedere il permesso ai genitori o agli insegnanti: infatti, non si può avere la certezza dell'identità della persona con la quale si sta comunicando.
12. Non prendere appuntamenti con persone conosciute tramite web senza aver interpellato prima i genitori.
13. Non inviare fotografie tue o di altre persone.
14. Riferisci sempre ai tuoi genitori o ai tuoi insegnanti se incontri in Internet immagini o scritti che infastidiscono.
15. Se qualcuno non rispetta queste regole, è opportuno parlarne con gli insegnanti o con i genitori.
16. Chiedi il permesso prima di scaricare dal web materiale di qualsiasi tipo.

La violazione deliberata di queste norme determinerà la rimozione temporanea o permanente del tuo account, cioè dei servizi che ti sono stati messi a disposizione.

4 PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

La scuola è una comunità di dialogo, di ricerca, di esperienza sociale, informata ai valori democratici e volta alla crescita della persona in tutte le sue dimensioni. In essa ognuno, con pari dignità nella diversità dei ruoli, opera per garantire la formazione alla cittadinanza, la realizzazione del diritto allo studio, lo sviluppo delle potenzialità di ciascuno e il recupero delle situazioni di svantaggio, in armonia con i principi sanciti dalla Costituzione e dalla Convenzione internazionale sui diritti dell' infanzia istituita a New York il 20 novembre 1989 e con i principi generali dell'ordinamento italiano (DPR 24 giugno 1998, n. 249).

4.1 Prevenzione

Il primo passo che la nostra scuola intraprenderà sarà quello di coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online. I casi rilevati saranno gestiti affrontando il problema sotto diversi punti di vista.

In primo luogo s'informeranno gli alunni sulle conseguenze riguardanti il fenomeno emerso; in seguito si cercherà di aiutare l'alunno coinvolto e vittima creando situazioni di dialogo che consentano di far emergere gli aspetti di criticità per i quali, attraverso un confronto, si potrà intervenire.

Internet, pur essendo una grande opportunità di crescita e ampliamento delle proprie conoscenze, presenta infatti, potenziali rischi per alcuni soggetti, come i minori, che non riescono ad assumere un atteggiamento critico verso di esso.

Per questo motivo se ne promuove l'uso critico e consapevole da parte degli utenti, e si ostacolano le pratiche di abuso dello strumento, anche attraverso un'autoregolamentazione interna, ponendo attenzione alla rilevazione di rischi connessi alla navigazione sul web (cyberbullismo, adescamento online, sexting, pornografia, pedopornografia, gioco d'azzardo, dipendenza, esposizione a contenuti dannosi o inadeguati.)

Il nostro Istituto ha scelto una politica interna pro-attiva, tesa a creare un ambiente di apprendimento sereno e sicuro, in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi; in cui ci sia l'apertura necessaria all'incoraggiamento a parlare di sé e dei propri problemi; che stimoli alla partecipazione diffusa di tutta la comunità scolastica nelle azioni finalizzate al contrasto del (cyber)bullismo; che insegni ad interagire in maniera responsabile.

Contrastare il bullismo implica la creazione di una comunità solidale, in cui ogni allievo accetta sia il diritto di vivere una scuola senza violenza, sia la responsabilità di difendere i compagni più vulnerabili. Il coinvolgimento dei coetanei è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto, sottrarre al bullo i potenziali proseliti.

4.1.2 Azioni

Nel corso del triennio della Policy, l'istituto ha realizzato e realizzerà:

1. attività di peer education

2. attività inerenti al progetto "Generazioni connesse"

3. diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e contrasto al bullismo e cyberbullismo del MIUR e del relativo aggiornamento

4. proposte di approccio curricolare, inserendo attività di sensibilizzazione nell'azione didattica, da svolgere in classe a cura dei docenti, utilizzando filmati, episodi di cronaca recenti o testi come stimolo per la discussione in classe, l'acquisizione di consapevolezza del problema, delle motivazioni sottostanti e delle conseguenze e lo sviluppo di un sistema di regole e di una cultura anti prepotenze nella classe.

5. implementazione dell'e-Safety Policy, con il contributo di tutte le componenti (docenti, studenti, famiglie, personale ATA)

6. presentazione dell'e-Safety Policy così redatta agli Organi Collegiali, condivisione, approvazione e integrazione nei regolamenti d'istituto e relativa pubblicazione sul sito istituzionale.

4.2 Rilevazione

4.2.1 Che cosa segnalare

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti: I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni online, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante.

Una prova di quanto riferito può essere presente nei dispositivi tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso; se da un lato il docente è autorizzato a monitorare le strumentazioni della scuola, dall'altro è tenuto a rivolgersi ai genitori per controllare l'uso del telefono cellulare.

I contenuti pericolosi comunicati/ricevuti a/ da altri, messi/ scaricati in rete, in altre parole, le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola dai minori (l'eventuale telefonino/smartphone personale e il PC collegato a Internet) per gli alunni sono relativi a:

- offese e insulti tramite messaggi di testo, e-mail, pubblicati sui social network o tramite telefono (ad esempio telefonate mute);
- diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network
- esclusione dalla comunicazione online, dai gruppi
- furto, appropriazione, uso e rilevazione ad altri, di informazioni personali come le credenziali d'accesso all'account e-mail, social network…..

4.2.2 Come gestire le segnalazioni

Una volta ricevuta una segnalazione di abuso, le tappe da seguire sono:

- se possibile fermare immediatamente l'abuso
- dare sostegno alla vittima
- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento
- dare supporto al bullo con un programma educativo che si focalizzi su due fronti: il coinvolgimento attivo del gruppo dei pari per sviluppare l'empatia e l'intervento dei docenti per gestire l'aggressività e la rabbia

Come per la prevenzione, il coinvolgimento dei coetanei è indispensabile per garantire l'efficacia dell'intervento finalizzato a:

- creare un clima di solidarietà
- combattere l'indifferenza e la deresponsabilizzazione morale
- incoraggiare le vittime a chiedere aiuto
- sottrarre al (cyber)bullo potenziali proseliti

La scuola, poiché comunità scolastica solidale si dichiara contraria a ogni forma di (cyber)bullismo, monitorando i casi segnalati, mediante la compilazione di un documento in cui registrare i casi verificatisi.

4.3 Legge n.71/2017 *"Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyber bullismo"*

Il 17 maggio 2017 la Camera dei Deputati ha approvato in via definitiva, senza ulteriori modifiche, la proposta di legge A.C. 3139-B, volta alla prevenzione e al contrasto del fenomeno del (cyber)bullismo.

La Legge n. 71/2017 introduce una serie di misure di carattere educativo e formativo, finalizzate in particolare una maggiore consapevolezza tra i giovani del disvalore dei comportamenti persecutori che, generando spesso isolamento ed emarginazione, possono portare a conseguenze anche molto gravi su vittime in situazione di particolare fragilità

In sintesi, il contenuto della legge:

- individua la finalità dell'intervento nel contrasto del cyber bullismo in tutte le sue manifestazioni attraverso una strategia che comprende misure di carattere preventivo ed educativo nei confronti dei minori (vittime e autori del bullismo sul web) da attuare in ambito scolastico;
- prevede che il minorenne che abbia compiuto 14 anni e sia vittima di bullismo informatico (nonché ciascun genitore o chi esercita la responsabilità sul minore) possa rivolgere istanza

al gestore del sito Internet o del social media o, comunque, al titolare del trattamento per ottenere provvedimenti inibitori e prescrittivi a sua tutela (oscuramento, rimozione, blocco di qualsiasi altro dato personale del minore diffuso su Internet, con conservazione dei dati originali). Il titolare del trattamento o il gestore del sito Internet o del social media deve comunicare, entro 24 ore dall'istanza, di avere assunto l'incarico e deve provvedere sulla richiesta nelle successive 48 ore. In caso contrario, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali che deve provvedere, in base alla normativa vigente, entro le successive 48 ore;

- istituisce un tavolo tecnico per la prevenzione ed il contrasto del cyber bullismo e prevede l'adozione, da parte del MIUR, sentito il Ministero della giustizia, di apposite linee di orientamento – da aggiornare ogni due anni – per la prevenzione ed il contrasto del cyber bullismo nelle scuole. In particolare, le linee di orientamento dovranno prevedere una specifica formazione del personale scolastico, la promozione di un ruolo attivo degli studenti e la previsione di misure di sostegno e rieducazione dei minori coinvolti;
- prevede la designazione, in ogni istituto scolastico, di un docente con funzioni di referente per le iniziative contro il cyberbullismo, il quale dovrà collaborare con le Forze di polizia, con le associazioni e con i centri di aggregazione giovanile presenti sul territorio;
- prevede interventi di carattere educativo in materia di cyber bullismo (finanziamento di progetti e promozione dell'uso consapevole di Internet);
- in caso di episodi di cyber bullismo in ambito scolastico, prevede inoltre l'obbligo da parte del Dirigente di informare tempestivamente i genitori (o i tutori) dei minori coinvolti e di attivare adeguate azioni educative;
- applica la disciplina sull'ammonimento del questore, mutuata da quella dello stalking, anche al cyberbullismo: fino a quando non sia stata proposta querela o presentata denuncia per i reati di ingiuria,diffamazione, minaccia o trattamento illecito di dati personali commessi, mediante Internet, da minorenni ultraquattordicenni nei confronti di altro minorenne, il questore – assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti – potrà convocare il minore responsabile (insieme ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale), ammonendolo oralmente ed invitandolo a tenere una condotta conforme alla legge.

4.4 Gestione dei casi: cosa fare in caso di… cyberbullismo?

SCHEMA DI INTERVENTO IN CASO DI CYBERBULLISMO

(AGGIORNATO LEGGE 71/2017)

Tratto da http://piattaforma.generazioniconnesse.it/mod/resource/view.php?id=172

Cosa fare in caso di… Cyberbullismo?

CASO A (SOSPETTO) – Il docente sospetta che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

ATTORI ADULTI DA COINVOLGERE

- Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.
- Valuta se è il caso di avvisare i Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.
- Dialoga con i colleghi/e: confrontati, condividendo le tue preoccupazioni.
- Raccogli le informazioni, ascoltando i ragazzi e monitorando ciò che accade
- Capire il livello di diffusione dell'episodio a livello di Istituto

CLASSE/I DA COINVOLGERE

Dialoga con la classe: Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggerisci di **chiedere aiuto** per situazioni di questo tipo. Prevedi un momento laboratoriale (suggerimenti utili nel corso 1)

Se ancora non ci sono evidenze, previeni:

lavora con la classe sul clima: Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Informa gli alunni su ciò che dice **la legge italiana** sul cyberbullismo

Continua a monitorare la situazione

Promuovi per l'intera comunità scolastica percorsi di prevenzione dei comportamenti a rischio online

Cosa fare in caso di … cyberbullismo ?

CASO B (EVIDENZA) – Il docente ha evidenza che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

ATTORI ADULTI DA COINVOLGERE

1. **Condividi** con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.
2. **Avvisa** il Dirigente Scolastico, anche in base al regolamento interno, sarà sua cura allertare la polizia postale e/o le autorità competenti.
3. **Richiedi** la consulenza dello psicologo/a scolastico, se presente, a supporto della gestione della situazione, in base alla gravità
4. **Dialoga** con i colleghi/e: confrontati , condividendo le tue informazioni e strategie.
5. **Informa** i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete informazioni e strategie.
6. **Informa** i genitori di ragazzi/e della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
7. **Valuta** come coinvolgere gli operatori scolastici su quanto sta accadendo.

CLASSE/I DA COINVOLGERE

1. **Capire** il livello di diffusione dell'episodio a livello di Istituto e parla della necessità di non diffondere ulteriormente online i materiali.
2. **Dialoga** (con la classe – 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggerisci di **chiedere aiuto** per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.
3. **Dialoga** (con la classe – 2): a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni, rispetto al loro suolo, anche di spettatori, nella situazione.

Tieni traccia di quanto successo e delle azioni intraprese:
compila il diario di bordo

Questo documento è stato redatto dai docenti che hanno frequentato l'Unità Formativa realizzata dal nostro Istituto: "*Coesione sociale e prevenzione del disagio giovanile globale: azioni di prevenzione e di contrasto al bullismo e al cyberbullismo*". Relatore: Dott. Bilotto Andrea.

Baravelli Monia

Biondi Gabriella

Biserni Annalisa

Casadei Turroni Monti Sabrina

Colangelo Giuseppina Paolina

Corbi Daniela

Corzani Alba

Di Perna Teresa

Gabelli Afra

Giorgini Alessandra

Guida Maria Concetta

Landi Daniela

Mariani Paola

Messina Paola

Raggini Lorenzo

Ricci Vittoria

Scotti Maria Cristina

Tazzari Antonella