

**Istituto Comprensivo ad indirizzo musicale
Giacomo Matteotti
di Aprilia - LT**

MUSICA **Arte** **Laboratori** **Scienze** **Sport** **Digitale** **Concorsi** **Lingue Straniere** **Pon** **Sicurezza** **Viaggi d'istruzione** **Tradizione e Innovazione**

NEVER STOP LEARNING

e-learning Moodle

I.C. Matteotti - Sede Centrale - Via O. Respighi n°6 - Tel: 069257905 - Fax: 069257952
Orari di Ricevimento Segreteria Didattica: Lun. 8:30/9:30 Merc. 11:30/13:00 Giov. 13:00/14:30
IT15C0306914603100000046021 Itic824009@pec.istruzione.it

E- Safety Policy

a.s.2019/2020



Sommario

INTRODUZIONE	4
1. SCOPO DELLA POLICY	4
1.1 Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)	5
1.2 Condivisione e comunicazione della Policy all'intera comunità scolastica	10
1.2.1 Condividere e comunicare la politica di e-Safety agli alunni	11
1.2.2 Condividere e comunicare la politica di e-Safety al personale.....	11
1.2.3 Condividere e comunicare la politica di e-Safety ai genitori	11
1.3 Gestione delle infrazioni alla Policy	11
1.3.1 Disciplina degli alunni	11
1.3.2 Disciplina del personale scolastico	12
1.3.3 Disciplina dei genitori	13
1.4 Monitoraggio dell'implementazione della Policy e suo aggiornamento	13
2. FORMAZIONE E CURRICOLO DIGITALE	13
2.1 Curricolo sulle competenze digitali per gli studenti	13
2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica	19
2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle Tecnologie Digitali	20
2.4 Sensibilizzazione delle famiglie	20
3. GESTIONE DELL'INFRASTRUTTURA, DELLA STRUMENTAZIONE ICT DELLA SCUOLA, COMPRESI I TABLET IN COMODATO D'USO PER LA DAD, E DELLA STRUMENTAZIONE PERSONALE	21
3.1 Regolamento per l'utilizzo del laboratorio di informatica e la navigazione Internet.....	22
3.1.1 Norme generali di comportamento.....	22
3.1.2 Uso di Internet.....	23
3.1.3 Utilizzo delle stampanti	23
3.2 Principali norme per gli insegnanti e per gli studenti sull'utilizzo della Piattaforma Moodle e OFFICE 365 Tratto da: GRIGLIA DI VALUTAZIONE DIDATTICA A DISTANZA: SCUOLA SEC. DI I GRADO Indicazioni e modalità operative per videolezioni – Buone pratiche Videolezioni online	24
3.2.1 Principali norme per gli insegnanti	24
3.2.2 Partecipazione alle videolezioni online	24
3.2.3 Norme per lo studente	24
3.3 Accesso a Internet: filtri, antivirus e sulla navigazione.....	27

3.4 Disposizioni sull'uso dei software.....	28
3.5 Gestione accessi (password, backup, ecc.).....	28
3.6 E-mail	28
3.7 Sito web della scuola	29
3.8 Social network	29
3.9 Protezione dei dati personali.....	30
3.10 Strumentazione personale: gestione degli strumenti personali – cellulari, tablet ecc.	30
3.10.1 Per gli studenti.....	30
3.10.2 Per i docenti.....	31
3.10.3 Per il personale della scuola	31
4. PREVENZIONE E RILEVAZIONE	31
4.1 Prevenzione	31
4.1.1 Rischi.....	33
4.1.2 Azioni	34
4.2 Rilevazione.....	35
5. SEGNALE E GESTIONE DEI CASI.....	36
5.1 Cosa segnalare	36
5.2 Come segnalare: quali strumenti e a chi	38
5.2.1 Strumenti a disposizione di studenti/esse.....	38
5.3 Gli attori sul territorio.....	38
5.4 Allegati con procedure schede di segnalazione e diario di bordo.....	41
ANNESI	46
1.LINEE GUIDA PER UNA SCUOLA LIBERA DA CYBERBULLISMO	46
1.1 LINEE GUIDA PER I RAGAZZI	46
1.2 LINEE GUIDA PER I GENITORI.....	46
1.3 LINEE GUIDA PER LA SCUOLA	46

INTRODUZIONE

Nell'ambito del progetto "Generazioni connesse" (www.generazioniconnesse.it) a cui il nostro Istituto ha aderito da tempo, è stato elaborato questo documento programmatico anche in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione. Non si tratta di un documento meramente formale, poiché a partire da esso la scuola intende promuovere:

- la formazione rivolta al personale interno circa le tematiche previste dalla policy;
- l'impegno di tutti gli attori coinvolti nel rispetto di quanto definito nel documento;
- l'adeguamento del curriculum per ottemperare a quanto stabilito nella policy;
- la sensibilizzazione dei genitori sul tema della sicurezza online;
- dei partenariati con enti e associazioni esterne.

Internet è un'inestimabile risorsa per l'educazione e l'informazione, offre infinite opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati e mettere in comune esperienze. Da un punto di vista amministrativo, grazie all'implementazione costante del sito Internet della scuola, all'introduzione del registro elettronico Axios e della piattaforma Collabora, all'utilizzo delle piattaforme Moodle e Microsoft Teams 365, a cui possono accedere Dirigente, docenti, personale amministrativo, alunni, è diventato più semplice gestire il nostro sistema-scuola e aprire la scuola all'utenza con una comunicazione più tempestiva, chiara e trasparente.

Allo stesso tempo, l'uso sempre più pervasivo di piattaforme in rete e dispositivi portatili ha esposto gli utenti e in particolare i minori, i soggetti con divario digitale o con limitate competenze informatiche a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni rese possibili.

L'obiettivo è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet, gestire problematiche connesse ad un uso non consapevole delle tecnologie digitali e promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR.

1. SCOPO DELLA POLICY

Scopo del presente documento è di informare l'intera comunità scolastica per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

In particolare, l'intento della scuola è di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di Internet, di far acquisire loro procedure e competenze "tecniche", ma anche corrette norme comportamentali, di prevenire, in altre parole rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

Gli utenti devono essere pienamente consapevoli dei rischi cui si espongono quando navigano in rete. Pertanto, la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. In questo contesto, gli Insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa per prevenire il verificarsi di situazioni potenzialmente pericolose.

1.1 Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)

I ruoli e le responsabilità assunti dagli attori della comunità scolastica seguono tre linee d'intervento volte a promuovere l'uso consapevole e corretto delle tecnologie e di Internet, di seguito riportate:

1. aggiornamento dell'e-Safety Policy d'Istituto, in altre parole del proprio codice di condotta nella prevenzione e gestione dei casi di (cyber)bullismo e del regolamento di sicurezza informatica che ha preso come riferimento i principi proposti dal MIUR nel documento che riassume "La posizione italiana sui principi fondamentali di Internet";
2. promozione della cittadinanza digitale, con la valorizzazione negli allievi della competenza digitale e della cultura del rispetto di regole comuni nell'uso dei servizi telematici e con lo sviluppo di regole di buon comportamento (Netiquette), riferite specialmente ai Social Network e al loro uso responsabile e informato;
3. adozione di procedure condivise per la gestione delle problematiche e realizzazione di attività per la prevenzione dei rischi articolate con interventi nelle classi.

Pertanto, si riconoscono, in ciascun ruolo, le seguenti responsabilità:

RUOLO	RESPONSABILITÀ
<i>Dirigente Scolastico</i>	• responsabilità generale per la sicurezza dei dati; • garantire l'uso di un Internet service conforme alle normative vigenti; • responsabilità di garantire adeguata formazione al personale in merito alla sicurezza online; • conoscere le procedure da seguire in caso di infrazione dell'e-Safety Policy; • ruolo di primo piano nello stabilire e rivedere l'e-Safety Policy; • ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; • garantire un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online;

	• gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali; • culpa in organizzando: si riferisce ai provvedimenti previsti e presi dal dirigente scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
Responsabili 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; • assumere la responsabilità per (aggiornarsi e monitorare) i problemi di sicurezza online; • promuovere la consapevolezza e l'impegno per la protezione online dell'intera comunità scolastica; • 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; • mantenere agli atti un registro di incidenti di sicurezza online; • favorire la formazione e la consulenza a tutto il personale; • coordinare le attività della scuola con le autorità locali e le agenzie competenti; • controllare l'accesso a materiali illegali/inappropriati; • controllare eventuali azioni di cyberbullismo.
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 alle 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 progetti attinenti la "scuola digitale".
Referente Cyberbullismo	• il referente ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio; • promuovere attività o progetti da svolgere nelle classi; • applicare e controllare i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber/bullismo; • coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti l'utilizzo consapevole di Internet; • svolgere un importante compito di supporto al Dirigente Scolastico per la revisione/stesura di regolamenti (regolamento d'istituto), atti e documenti (PTOF, PDM, RAV).
Docenti	• 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; • garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche e educative delle classi; • garantire che gli alunni capiscano e seguano le 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 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 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; • 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); • guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet 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 esigenze 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 riguardo all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme; • culpa in vigilando: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (così come da art. 2048 del c.c.). tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").
Personale Amministrativo Tecnico ed Ausiliario (ATA)	• 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; • essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.
Alunni	• leggere, comprendere, accettare e applicare l'e-Safety Policy; • 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 ma anche della necessità di 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; • concordare con i docenti linee d'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; • tenere sotto controllo e monitorare l'uso che i figli fanno di Internet e del telefonino in generale; • culpa in educando: fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.
<i>Gli Enti educativi esterni e le associazioni</i>	• gli enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della rete e delle TIC; • devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

1.2 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, alla sua stesura hanno collaborato genitori, alunni e tutto il personale della scuola. Sono state sottoscritte da tutti i soggetti coinvolti nella loro redazione, sono state portate a conoscenza degli Organi Collegiali e di tutti gli operatori e gli utenti della scuola: con questo documento s'intende attivare e mantenere nella nostra scuola un'e-Safety Policy in materia di tecnologie dell'informazione e della comunicazione condivisa e accettata da tutti.

1.2.1 Condividere e comunicare la politica di e-Safety agli alunni

Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.

L'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla rete.

Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni sono più esposti o rispetto ai quali sono più vulnerabili.

1.2.2 Condividere e comunicare la politica di e-Safety al personale

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà discussa negli organi collegiali (consigli di classe/interclasse/intersezione, collegio dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web.

Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali.

Il personale docente sarà reso consapevole del fatto che il traffico in Internet può essere monitorato e si potrà risalire al singolo utente registrato.

Un'adeguata informazione/formazione online del personale docente nell'uso sicuro e responsabile di Internet, sia professionalmente sia personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola.

Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

1.2.3 Condividere e comunicare la politica di e-Safety ai genitori

L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di Internet sarà attirata sul sito web della scuola nell'area a essi dedicata.

Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia.

Si forniranno ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet anche a casa.

1.3 Gestione delle infrazioni alla Policy

1.3.1 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. Infatti, più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto. Tali atteggiamenti vanno compresi e orientati dagli educatori al raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente Scolastico;
- la sospensione.

Contestualmente sono 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 di amicizia, di sviluppo della conoscenza e della gestione delle emozioni.

1.3.2 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 di 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 carente 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.

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 della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

1.3.3 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 o 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 oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero essere pericolosi per sé e/o dannosi per gli altri.

1.4 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto periodicamente e sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti alla fine dell'anno, riguardo all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente Scolastico o da un docente Referente appositamente designati, dall'Animatore Digitale, dagli Organi Collegiali, secondo gli aspetti considerati.

2. FORMAZIONE E CURRICOLO DIGITALE

2.1 Curricolo sulle competenze digitali per gli studenti

“La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza, spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” (“Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente”, C189/9, p.9).

Lo sviluppo di una piena cittadinanza digitale passa attraverso la capacità degli studenti di appropriarsi dei media digitali, passando da consumatori passivi a consumatori critici e produttori responsabili di contenuti e può considerarsi suddivisa in quattro aree:

Area 1: “Alfabetizzazione e dati”

L’area riguarda la capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete al fine di acquisire le seguenti competenze:

- navigare, ricercare e valutare informazioni e contenuti digitali;
- saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete.

Area 2: “Comunicazione”

L’area sviluppa la competenza di comunicare e relazionarsi online, in particolare:

- saper interagire con gli altri attraverso le tecnologie digitali;
- essere consapevoli nella condivisione delle informazioni in Rete;
- conoscere le “Netiquette”, ovvero le norme di comportamento online;
- saper gestire la propria “identità digitale”.

Area 3: “Creazione di contenuti digitali”

Quest’area sviluppa le seguenti specifiche competenze digitali:

- creare e modificare contenuti digitali in diversi formati;
- essere consapevoli che le risorse su Internet possono essere coperte da copyright.

Area 4: “Sicurezza”

Quest’area è parte di una dimensione più generale definita come “benessere digitale” che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui.

CURRICOLO VERTICALE DIGITALE: SCUOLA DELL’INFANZIA, PRIMARIA, SECONDARIA

La competenza digitale coinvolge tutti gli insegnanti e tutte le discipline sono coinvolte e concorrono alla sua costruzione. Per i docenti, impegnati in questa rivoluzione tecnologica, si tratta di sperimentare una didattica integrata e innovativa che riconosca il ruolo degli strumenti digitali e favorisca l’uso consapevole della tecnologia e l’inclusione. L’aula, attraverso la rete, si apre al mondo e la progettazione didattica della scuola si orienta ad una completa integrazione della tecnologia nel processo di apprendimento.

AREE di COMPETENZA	DESCRIPTORI di COMPETENZA
ALFABETIZZAZIONE E DATI	L'alunno: ricerca, conserva, organizza e analizza le informazioni digitali.
COMUNICAZIONE	L'alunno: comunica in ambienti digitali, condivide risorse attraverso strumenti on-line, sa collegarsi con gli altri e collabora attraverso strumenti digitali, interagisce e partecipa alle comunità e alle reti.

CREAZIONE DI CONTENUTI	L'alunno: crea e modifica contenuti, integra e rielabora conoscenze, produce espressioni creative.
SICUREZZA	L'alunno: riflette e acquisisce consapevolezza su protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile
Dal "Quadro di riferimento per le competenze digitali dei cittadini europei" - (Framework EQF sulle DIGICOMP)	COMPETENZA CHIAVE: competenza digitale (revisione Consiglio Europeo, maggio 2018) "La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico". PROFILO DELLO STUDENTE AL TERMINE DEL PRIMO CICLO DI ISTRUZIONE (Indicazioni Nazionali 2012): "L'alunno ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati e informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo."

TRAGUARDI FORMATIVI		
Al termine della Scuola dell'INFANZIA	Al termine della Scuola PRIMARIA	Al termine della Scuola SECONDARIA di I grado
Padroneggiare prime abilità di tipo logico, iniziare a interiorizzare le coordinate spazio-temporali e ad orientarsi nel mondo dei simboli, delle rappresentazioni, dei media, delle tecnologie.	- Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. - Utilizzare con dimestichezza e spirito critico le nuove tecnologie. - Usare il computer e la rete per reperire, valutare, produrre, presentare, scambiare informazioni. - Riflettere sulle potenzialità, i limiti e i rischi dell'uso delle	- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. - Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago. - Conoscere le caratteristiche e le potenzialità tecnologiche degli strumenti d'uso

	tecnologie dell'informazione e della comunicazione.	più comuni. Riconoscere vantaggi, potenzialità, limiti e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.
--	---	--

OBIETTIVI DI APPRENDIMENTO SCUOLA DELL'INFANZIA – ALUNNI SEZIONE 5 ANNI

- Avvicinare il bambino alla curiosità dell'utilizzo del computer.
- Sviluppare la coordinazione oculo-manuale.
- Arricchire il vocabolario di termini tecnologici.
- Saper avviare e spegnere il computer
- Saper direzionare il movimento del mouse in relazione a quanto appare sul monitor.
- Comprendere il concetto di causa-effetto.
- Saper utilizzare i principali tasti della tastiera.
- Sviluppare la fantasia attraverso programmi di grafica.

OBIETTIVI DI APPRENDIMENTO SCUOLA PRIMARIA

Al termine della classe prima	Al termine della classe seconda	Al termine della classe terza	Al termine della classe quarta	Al termine della classe quinta
Accendere e spegnere il computer e la Lim. Conoscere le principali parti del computer e loro funzioni (monitor, tastiera, CPU, mouse). Saper utilizzare semplici programmi per disegnare e giochi didattici. Scrivere lettere, semplici parole e semplici frasi con programma di videoscrittura. Utilizzare correttamente il mouse.	Accendere e spegnere in modo corretto il computer e la Lim. Utilizzare il mouse per dare alcuni semplici comandi al computer. Usare i principali comandi della tastiera. Aprire e chiudere un file. Aprire e chiudere un'applicazione. Utilizzare programmi di videoscrittura e disegno. Usare software	Accendere e spegnere in modo corretto il computer e la Lim. Utilizzare il mouse e tastiera. Creare una cartella personale. Salvare con nome in una cartella e/o su supporto removibile. Aprire e chiudere un file. Aprire e chiudere un'applicazione. Utilizzare i primi elementi di formattazione (impostare il carattere e	Utilizzare semplici programmi per elaborare mappe utili per lo studio. Usare corsivo, grassetto e sottolineatura. Colorare un testo. Usare i comandi di allineamento e di giustificazione del testo. Usare la formattazione del paragrafo. Inserire elenchi puntati. Usare il programma di videoscrittura. Usare software	Inserire bordi e sfondi Utilizzare la barra del disegno. Inserire WordArt e Clipart. Utilizzare la rete per scopi di informazione, comunicazione (email...), ricerca e svago. Conoscere potenzialità e rischi connessi all'uso delle tecnologie informatiche. Costruire la linea del tempo in forma digitale. Usare il programma di videoscrittura.

Utilizzare tastiera.	la	didattici.	allineare il testo) per scrivere brevi testi. Usare software didattici. Eseguire ricerche, on line, guidate. Costruire la linea del tempo in forma digitale. Prendere visione del foglio di calcolo di Excel e delle sue principali funzioni	didattici. Eseguire ricerche, on line, guidate. Costruire la linea del tempo in forma digitale. Usare software di geometria (Dècllic, GeoGebra ...) Gestire righe e colonne di Excel. Inserire i dati nel foglio di lavoro. Conoscere PowerPoint e le sue funzioni principali	Utilizzare il controllo ortografico e grammaticale. Inserire tabelle. Usare software di geometria (Dècllic, GeoGebra ...) Navigare in Internet, attraverso un browser, in alcuni siti selezionati. Conoscere i più comuni motori di ricerca. Creare un grafico con Excel. Creare una diapositiva con PowerPoint inserendo immagini e/o audio e/o video. Creare un ipertesto.
----------------------	----	------------	---	--	--

OBIETTIVI DI APPRENDIMENTO SECONDARIA DI I GRADO

Al termine della classe prima	Al termine della classe seconda	Al termine della classe terza
Scrivere, formattare, revisionare e archiviare, in modo autonomo, testi scritti con il computer Salvare i documenti. Utilizzare semplici programmi di grafica. Creare diapositive digitali inserendo immagini, audio, video. Manipolare e modificare i testi prodotti, inserendo elementi grafici. Utilizzare i dizionari digitali. Elaborare e costruire semplici tabelle di dati e grafici con la supervisione dell'insegnante. Usare software di geometria. Introdurre il rapporto tra pensiero computazionale, algoritmi e coding. Conoscere le procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, e-mail, chat, social network, protezione degli account, download, diritto d'autore, ecc.). Utilizzare una piattaforma (come MOODLE e OFFICE 365) per l'accesso alle informazioni e agli usi per le quali è stata creata e utilizzata nella didattica. Proteggere i dati personali e la privacy. Riconoscere contenuti pericolosi o fraudolenti nella rete (spam, falsi messaggi di posta, richieste	Conoscere le procedure per la produzione di testi, presentazioni e utilizzo dei fogli di calcolo. Creare diapositive e racconti digitali inserendo immagini, audio, video (storytelling). Utilizzare i dizionari digitali. Utilizzare il foglio elettronico Excel per costruire tabelle e grafici di vario tipo. Utilizzare i necessari software per editing video, elaborazione testi, suoni e immagini, disegno tecnico. Usare software di geometria. Fruire di video e documentari didattici in rete. Conoscere il rapporto tra pensiero computazionale, algoritmi e coding. Proteggere i dispositivi. Proteggere i dati personali e la privacy. Conoscere le procedure di utilizzo della rete per ottenere dati, fare ricerche, comunicare.	Conoscere e utilizzare in autonomia programmi di videoscrittura, presentazioni, disegni, per comunicare, eseguire compiti. Creare diapositive e racconti digitali inserendo immagini, audio, video (storytelling). Utilizzare il foglio elettronico Excel per costruire tabelle e grafici statistici di vario tipo. Realizzare ipertesti utilizzando gli applicativi più comuni. Utilizzare i necessari software per editing video, elaborazione testi, suoni e immagini e per disegno tecnico. Usare software di geometria. Scrivere sequenze di comandi per inventare una storia o un gioco. Sviluppare il pensiero logico e algoritmico. Approfondire il rapporto tra pensiero computazionale, algoritmi e coding. Conoscere la struttura di base di un algoritmo ed i principali "blocchi logici" su cui si basano tutte le strutture di programmazione.

di dati personali, ecc.).		
Fruire di video e documentari didattici in rete.		

SOFTWARE E APPLICATIVI PER CREARE PERCORSI NEL DIGITALE

SCUOLA dell'INFANZIA

Giochi per imparare a maneggiare il mouse.
 Un gioco per memorizzare la posizione dei tasti sulla tastiera del computer.
 Giochi ed esercizi di tipo logico, linguistico, matematico, topologico, al computer.
 Visionare immagini, brevi filmati e documentari didattici.
 Ricomporre un'immagine virtuale, per trascinalamento delle varie parti costitutive.
 Un programma di disegno progettato per bambini, con tecniche molto semplici.

SCUOLE PRIMARIA e SECONDARIA di I GRADO

La conoscenza dei programmi principali per la scrittura, la presentazione, il calcolo e il disegno costituisce la base per poter sperimentare le numerosissime App didattiche disponibili on line. La competenza nelle funzioni base di questi programmi, infatti, rende possibile l'adozione e l'utilizzo di altre applicazioni, sempre più complesse e strutturate.

Pertanto, per conseguire gli obiettivi di apprendimento e acquisire le competenze digitali nei diversi ordini di scuola, tutti i docenti possono scegliere di usare, sulla base delle proprie esigenze, competenze e discipline, i seguenti software e applicativi per tutte le discipline:

Produzione digitale di un testo (Word...)

Presentazioni digitali a supporto di un'esposizione (PowerPoint, Powtoon, Scratch...)

Realizzazione di ipertesti con possibilità di inserimento immagini, filmati, mappe concettuali, tabelle, per relazionare argomenti (PowerPoint, Prezi...)

Digital Storytelling

Dizionari digitali

Fruizione di video didattici in rete (Youtube, OVO, Zanichelli, RAI Scuola,...)

Verifica e autoverifica: quiz e test a risposta multipla, Vero/Falso, a risposta breve, sondaggi on line (Google moduli, Moodle, Office 365)

Piattaforme per consultare, condividere archiviare (Drive, Padlet, Moodle, Office 365)

Mappe concettuali (CMap Tools...)

Libri digitali e audiolibri

App per le lingue straniere

Foglio di calcolo per elaborazione numerica e grafica di dati (Excel)

Atlante digitale, Google maps, Google earth

Approccio all'editing video (Windows Live Movie Maker, ...)

Software specifici per creare musica e suonare

Software specifici per matematica e geometria (Geogebra, Desmos)

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

La professione docente è complessa e richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, sono importanti nella didattica al fine di progettare, sviluppare e valutare i

processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva).

Pertanto, l'Istituto favorisce la partecipazione del personale ad iniziative di formazione proposte dalla scuola, in accordo con la rete scolastica del territorio (ambito 21), le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti, e sostiene anche quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

Le azioni formative realizzate sinora 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'Istituto, dall'ambito e dall'equipe territoriali. Particolare rilevanza, anche nella formazione dei docenti, ha assunto l'utilizzo della piattaforma Moodle nella scuola secondaria di I grado (posta nell'area e-learning Matteotti) e l'avvio della piattaforma Office 365 per la scuola primaria.

L'utilizzo delle piattaforme consente agli alunni di frequentare ambienti virtuali sicuri e controllati e ai docenti di partecipare a videoconferenze, riunioni collegiali e di trasferire documenti in modo sicuro. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica è in continua evoluzione e può 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; può comprendere altresì l'uso dei materiali (video tutorial) messi a disposizione dall'Animatore stesso sulle bacheche virtuali presenti sul sito istituzionale, appositamente create, e di corsi di aggiornamento online.

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

La scuola ha partecipato (e continuerà a farlo) al progetto "Generazioni connesse" per alunni, genitori e docenti, a incontri formativi organizzati dalla Polizia di Stato di Latina e dall'associazione MOIGE.

Viste le positive reazioni di studenti, docenti e genitori e data la necessità di implementare l'E-Safety Policy con il contributo di tutte le componenti, la Scuola prevede di organizzare per i prossimi anni scolastici occasioni di confronto fra docenti sulle strategie più opportune da adottare come promozione dell'utilizzo consapevole e sicuro di Internet e delle TIC e come misure di prevenzione primaria al (cyber)bullismo.

Alcuni docenti si sono formati sull'utilizzo consapevole e sicuro di Internet.

Inoltre, sul sito istituzionale www.icmatteottiaprilia.edu.it è stato predisposto un banner sul quale sono disponibili materiali informativi sulla sicurezza in Internet per l'approfondimento personale, sulle attività con gli studenti e sugli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, del sito "Generazioni connesse", ecc.

2.4 Sensibilizzazione delle famiglie

Allo scopo di educare all'uso consapevole della rete e imparare a riconoscere i rischi a esso legato si terranno nell'Istituto incontri di sensibilizzazione e di formazione per i genitori, finalizzati all'uso responsabile della Rete, alla prevenzione e alla lotta al bullismo e cyberbullismo, anche con la presenza di esperti esterni legati alle forze dell'ordine.

La scuola inoltre si impegna a informare adeguatamente i genitori sulle condotte che dovranno adottare nelle comunicazioni digitali con l'Istituto e con i docenti (es. e-mail, gruppo Whatsapp, sito della scuola etc.) e a offrire loro consigli sull'uso delle tecnologie nella comunicazione con i figli in orario scolastico e in generale in famiglia.

3. GESTIONE DELL'INFRASTRUTTURA, DELLA STRUMENTAZIONE ICT DELLA SCUOLA, COMPRESI I TABLET IN COMODATO D'USO PER LA DAD, E DELLA STRUMENTAZIONE PERSONALE

L'Istituto s'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 sempre è 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. È fatto divieto a tutti gli studenti di utilizzare o comunque tenere accesi il telefono cellulare e altri dispositivi elettronici (fotocamere, videocamere, I-Pod, Mp3...) di loro proprietà o in loro possesso, ai sensi dell'art. 3 del D.P.R. 249/98 (Statuto delle studentesse e degli studenti), senza l'autorizzazione del docente durante l'attività didattica.
2. È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di voci, dialoghi e suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo per scopi puramente didattici.
3. È altresì fatto divieto ai docenti, ai sensi della C.M. 362/98, di utilizzare telefoni cellulari, per uso personale, durante lo svolgimento di attività d'insegnamento.
4. È a discrezione del docente chiedere che i telefoni cellulari siano depositati sulla cattedra.
5. 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, essi sono tenuti al sequestro immediato dell'apparecchio (spento dallo studente) e alla sua consegna al Dirigente Scolastico o, in sua assenza, ai suoi collaboratori, e contestualmente alla segnalazione del nominativo dello studente e degli estremi dell'accaduto.
6. Il Dirigente Scolastico o, in sua assenza, i suoi collaboratori prendono in consegna l'apparecchio sequestrato (spento) e lo custodiscono nei locali della Dirigenza. Le apparecchiature saranno consegnate personalmente ai genitori.
7. 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.

I **provvedimenti disciplinari**, commisurati all'entità della mancanza commessa e con riferimento all'art.4 del D.P.R. 249/198, sono i seguenti:

- rimprovero verbale privato o in classe;
- ammonizione scritta sul registro di classe;
- sospensione temporanea dalle lezioni, fino a 6 giorni, con obbligo di presenza a scuola;
- allontanamento dalla comunità scolastica per periodi non superiori a quindici giorni;
- allontanamento dalla comunità scolastica per periodi superiori ai 15 giorni;
- allontanamento dalla comunità scolastica fino al termine dell'anno scolastico;
- esclusione dallo scrutinio finale o non ammissione all'esame di Stato conclusivo del corso di studi.

3.1 Regolamento per l'utilizzo del laboratorio di informatica e la navigazione Internet

L'utilizzo delle attrezzature deve essere unicamente legato a scopi DIDATTICI.

Gli studenti della scuola potranno accedere al locale solo se accompagnati da un docente.

L'utilizzo dei personal computer e delle attrezzature comporta l'accettazione incondizionata del presente regolamento. Il laboratorio è un luogo di lavoro e pertanto è soggetto al D.L 81 del 2008 sulla prevenzione e la sicurezza del lavoro. Per la prevenzione degli incendi e il piano di evacuazione si fa riferimento alle disposizioni valide per l'intero Istituto.

All'interno del laboratorio deve essere depositata la seguente documentazione:

- regolamento
- orario settimanale del laboratorio
- registro firme e segnalazioni.

3.1.1 Norme generali di comportamento

1. Il laboratorio è a disposizione di tutte le classi dal lunedì al venerdì.
2. Ogni insegnante è tenuto ad aprire e chiudere l'aula mediante richiesta diretta e riconsegna delle chiavi ai collaboratori scolastici. Non è ammessa la consegna delle chiavi agli alunni.
3. È compito del docente compilare dettagliatamente e in ogni parte un apposito registro posto all'interno dell'aula di informatica.
4. Sul registro devono essere annotati la classe, l'insegnante accompagnatore e le eventuali difficoltà riscontrate (PC mal funzionanti, ...).
5. Ogni insegnante è tenuto a procedere all'accensione dei computer e all'iniziale verifica dell'integrità dei sistemi.
6. In laboratorio non è consentito consumare cibi e bevande di alcun tipo. Nell'eventualità della coincidenza con la ricreazione gli alunni sono obbligati a uscire dall'aula computer, consumare la propria merenda e rientrare a ricreazione ultimata.
7. All'uscita è cura del docente e degli alunni risistemare tastiere, mouse, sedie e quant'altro come sono stati trovati all'ingresso.
8. Gli alunni sono tenuti a rispettare le consegne dell'insegnante sull'utilizzo dei computer.
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 evenienza, situazione anomala, irregolarità rispetto al presente regolamento e malfunzionamento dell'attrezzatura, in particolare la presenza di software illegale o la presenza di contenuti non idonei, va 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.

3.1.2 Uso di Internet

1. La ricerca su Internet e l'uso della posta elettronica sono destinate alle finalità didattiche, scientifiche e di ricerca.
2. Tutte le macchine del laboratorio possono accedere a Internet.
3. Username e password di accesso a Internet sono assegnate solo al personale docente, gli alunni possono navigare su Internet solo sotto la diretta sorveglianza del docente, il docente non solo è tenuto a verificare continuamente la navigazione ma è anche direttamente responsabile dell'utilizzo di Internet da parte degli alunni cui ha dato la possibilità di collegarsi alla rete.
4. È compito dei docenti accompagnatori controllare i materiali scaricati dagli alunni durante la navigazione.

3.1.3 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 le motivazioni 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 del Laboratorio di informatica".
4. Ricordare agli allievi che se fosse rilevato un danno o comunque un malfunzionamento, si riterranno responsabili 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.

3.2 Principali norme per gli insegnanti e per gli studenti sull'utilizzo della Piattaforma Moodle e OFFICE 365 Tratto da: **GRIGLIA DI VALUTAZIONE DIDATTICA A DISTANZA: SCUOLA SEC. DI I GRADO** Indicazioni e modalità operative per videolezioni – Buone pratiche Videolezioni online

3.2.1 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 saranno forniti indirizzi di posta elettronica dal docente Animatore Digitale relativi ad account personali di Office 365, come ogni docente tutti gli alunni possiederanno un account con nome.cognome@icmatteottiaprilja.edu.it.
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.

3.2.2 Partecipazione alle videolezioni online

- a) I docenti sono consapevoli che l'obiettivo principale delle videolezioni online è mantenere attivo il rapporto docente-studenti e può rappresentare un momento qualificante della didattica a distanza.
 - b) I docenti utilizzano il proprio orario curricolare per calendarizzare le videolezioni.
 - c) I docenti, possono concordare con la propria classe eventuali sessioni pomeridiane.
 - d) I docenti registrano la partecipazione degli studenti alle videolezioni in orario curricolare (dal momento che la partecipazione rappresenta uno dei criteri per la valutazione in itinere e sommativa).
- I docenti possono utilizzare uno strumento personale per annotare le mancate partecipazioni o altri elementi utili alla valutazione. È anche possibile comunicare alla famiglia la mancata partecipazione attraverso Registro elettronico nella sezione Commento pubblico al voto. Linee guida comportamentali.

3.2.3 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, un tablet o uno smartphone
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. Non accedere ad altri account per copiare informazioni o compiti svolti.
4. Se utilizzi il tuo account su un dispositivo comune ricordati sempre di fare il logout

È indispensabile, per il regolare svolgimento di una video lezione e per ottenere una buona comunicazione in rete, rispettare le seguenti regole:

1. Essere puntuale: consulta l'orario settimanale per verificare i tuoi appuntamenti online e considera i tempi tecnici di collegamento
2. È vietato dare il link della video-lezione ad altri: l'aula virtuale è la tua classe, quindi, come in classe non possono entrare estranei o persone appartenenti ad altre classi.
3. Silenziare il cellulare quando ti colleghi, per evitare fonti di distrazione.
4. Disattivare il microfono ed attivarlo solo se richiesto dal docente (per rispondere all'appello o a domanda diretta).
5. Per intervenire chiedi la parola tramite chat o alzando la mano.
6. Non usare la chat per comunicare con i tuoi compagni, questo crea distrazione e rumore.
7. È necessario attivare la telecamera affinché il docente possa avere una visione d'insieme della classe.
8. Prima della lezione prepara sempre carta e penna, per essere pronto a prendere appunti.
9. È vietato scrivere, scarabocchiare o far comparire immagini sulla lavagna interattiva mentre il docente sta condividendo lo schermo e spiegando.
10. Non abbandonare il collegamento fino a quando il docente non dichiara terminata la lezione.
11. Le lezioni on line sono protette dalla privacy: è assolutamente vietato registrare, catturare screenshot dello schermo e diffonderle; la diffusione è perseguibile penalmente.

Norme per la salvaguardia della tua privacy e della tua sicurezza

1. Non comunicare mai il tuo username e la tua password a compagni o ad altre persone.
2. L'invio 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.

Come proteggere i tuoi dati quando utilizzi il pc, lo smartphone e il tablet per la DAD

Imposta il codice PIN e preferibilmente anche il codice di blocco in modo che non siano facilmente identificabili.

Conservare il codice IMEI utilizzabile per bloccare a distanza l'accesso al tuo smartphone o tablet in caso di furto o smarrimento.

Prima di dismettere un cellulare, un tablet o un PC i dati devono essere completamente cancellati: si può ripristinare le impostazioni di fabbrica, rimuovere la scheda sim e la scheda di memoria ed eliminare tutti i backup. Quando si scaricano applicazioni evitare fonti sconosciute e utilizzare market ufficiali.

Verificare che l'applicazione installata non richieda l'accesso ai dati personali (es. foto, rubrica...).

Leggere attentamente le condizioni d'uso per evitare di pagare servizi non richiesti o vedere esposte le informazioni personali.

Leggere con attenzione tutte le notifiche di accesso agli account, le notifiche sulle impostazioni di sicurezza e privacy.

Come proteggere i tuoi dati quando utilizzi lo smartphone e il tablet?

Utilizza i nomi di fantasia e non nomi reali perché esistono dei programmi che, utilizzando dizionari online, possono individuare facilmente il nome che hai scelto per la tua password.

Combina insieme maiuscole e minuscole, lettere, numeri caratteri speciali o simboli.

È importante cambiare la propria password periodicamente, non salvarla nel cellulare e non rivelarla a nessuno.

È importante non utilizzare la stessa password per account e siti diversi (es. profilo Facebook e posta elettronica): in caso di violazione su uno di essi, l'accesso non autorizzato automaticamente si potrebbe estendere agli altri

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

Normalmente occorre il permesso per riprodurre materiali quali testi, 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 far riferimento a materiale non coperto da copyright (vedi siti dedicati). Se ciò non è possibile devi comunque citare sempre la fonte dei materiali che utilizzi (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 e 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-.)

Norme di buona educazione in Internet (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, newsgroup, mailing list, forum, blog o e-mail.

In particolar modo devi rispettare le seguenti regole:

- se mandi un messaggio al tuo insegnante attraverso il forum è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema;
- non scrivere in maiuscolo tutto il messaggio, poiché ciò vorrebbe dire urlare nei confronti dell'interlocutore, cioè del destinatario del tuo messaggio;
- non divagare rispetto all'argomento del forum;
- non condurre "guerre di opinione" nel forum a colpi di messaggi e di contro-messaggi;
- 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.
- rispetta le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi;
- non fornire informazioni errate, imprecise, incomplete, ambigue e in caso di dubbio, verifica prima.
- non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
- l'invio e la ricezione di allegati alle e-mail devono eventualmente essere concordati con i genitori;
- richiedi sempre il permesso prima di iscriverti a qualche concorso, mailing-list o sito web che lo richieda;

- 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;
- non prendere appuntamenti con persone conosciute tramite web senza aver interpellato prima i genitori;
- non inviare fotografie tue o di altre persone;
- riferisci sempre ai tuoi genitori o ai tuoi insegnanti se incontri in internet immagini o scritti che infastidiscono;
- se qualcuno non rispetta queste regole, è opportuno parlarne con gli insegnanti o con i genitori;
- chiedi il permesso prima di scaricare dal web materiale di qualsiasi tipo.

Quali regole generali tenere a mente durante la navigazione in rete?

- non pubblicare informazioni personali e dati sensibili di altri utenti e non rendere pubblico un messaggio privato senza l'autorizzazione dell'autore, sia quando sei su un social (chiedi ad es. il consenso prima di taggare con foto e video) sia quando utilizzi mms o sistemi di messaggistica istantanea (es. Whatsapp o Messenger).
- non pubblicare foto che potrebbero mettere in una posizione di imbarazzo amici o in generale altri utenti.
- prima di diffondere informazioni accertati che siano esatte, verificale prima.
- quando pubblichi foto, video, frasi o parli di un libro, cita sempre la fonte o metti il link di riferimento.
- quando chiedi l'amicizia a qualcuno su un social che non è tuo amico, motiva la tua richiesta di amicizia.

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.

3.3 Accesso a Internet: filtri, antivirus e sulla navigazione

L'accesso a Internet è possibile e consentito per la didattica nei laboratori multimediali.

Nel laboratorio della scuola secondaria solo il docente dalla propria postazione può consentire agli alunni di accedere a Internet; Negli altri due plessi tutti i PC accedono ad Internet autonomamente (senza il consenso del docente.) Le postazioni non sono dotate di webcam.

L'animatore Digitale, il Team Digitale o il Responsabile del Laboratorio (uno per plesso) periodicamente provvedono alla manutenzione e aggiornamento del sistema informatico del laboratorio con il supporto e secondo le indicazioni e l'intervento di tecnici esterni. Le postazioni degli alunni sono occasionalmente utilizzate dai docenti, quando questi si servono dei laboratori. I docenti hanno piena autonomia nel collegamento ai siti web. Tuttavia, è necessario tenere presente che:

1. L'accesso a Internet è consentito al personale docente e non docente solo a esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. È vietato inserire sui PC connessi in rete programmi contenenti virus, scaricare software non autorizzati da Internet, scaricare e installare software senza licenza.

3.4 Disposizioni sull'uso dei software

1. I software installati sono a esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale.
3. È fatto divieto di usare software non conforme alle leggi sul copyright.

È cura dell'insegnante-utente di verificarne la conformità. Gli insegnanti non possono arbitrariamente installare un nuovo software sui PC del laboratorio ma dovranno rivolgersi ai tecnici responsabili che provvederanno all'installazione.

Per favorire e garantire a tutti la DAD, ogni alunno dell'I.C. sarà profilato per l'utilizzo gratuito della Piattaforma Office 365 e di tutte le app ad esso correlate, da cui potranno accedere da qualsiasi dispositivo, personale o scolastico.

3.5 Gestione accessi (password, backup, ecc.)

L'accesso al sistema informatico per la didattica, server e Internet, nel laboratorio multimediale è consentito al personale docente attraverso una password che è comune e consente di accedere al server. I docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati in ambiente cloud computing, di memorizzazione e sincronizzazione online. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

Accesso docenti:

- Ai docenti è consentito accedere a Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previa autorizzazione scritta del Dirigente;
- la connessione Wi-Fi a Internet dalla scuola è regolata da un meccanismo di autenticazione-autorizzazione munito di password;
- 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.
- il docente verificherà lo spegnimento della postazione al termine della sua ora di lezione.

Accesso studenti:

Il Regolamento di Istituto vieta l'uso del cellulare. Con la DAD consentiremo l'utilizzo del dispositivo solo per usi didattici. In particolare, agli studenti non è consentito accedere a Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.

3.6 E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi

didattici avverrebbe solo su autorizzazione del Dirigente Scolastico e operativamente sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

Solo i docenti possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici.

Prima di aprire una mail è necessario pensare a:

- Spam: e-mail, messaggi istantanei e altre comunicazioni online indesiderate.
- Phishing: frode online per sottrarre con l'inganno numeri di carte di credito, password, informazioni su account personali.
- Truffe: e-mail spedite da criminali che tentano di rubare denaro.

È importante effettuare la procedura di disconnessione dal proprio account personale, tutte le volte che si utilizza un dispositivo comune, di proprietà della scuola.

3.7 Sito web della scuola

La scuola ha un sito web. Tutti i contenuti del settore didattico e della segreteria sono pubblicati direttamente e sotto la supervisione dell'Animatore Digitale, che ne valuta con il Dirigente Scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Il Dirigente Scolastico e l'A.D. incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e agli utenti esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente.

3.8 Social network

Nella DAD è risultato utile e necessario anche l'utilizzo dei social network per la pubblicazione di informazioni, comunicazioni, attività legate alla didattica, per la condivisione con la componente genitoriale degli elaborati degli alunni. L'I.C. possiede una pagina Facebook di istituto gestita dall'A.D. e da altri 5 docenti della Scuola Primaria e Secondaria di Primo grado al fine di pubblicizzare le attività didattiche dell'istituto.

Nel periodo della Pandemia è iniziato anche uno scambio di file, messaggi e immagini tra docenti e alunni anche su WhatsApp, Piattaforme Didattiche come Collabora di Axios, WeeSchool, Padlet, Wiki, Google Classroom,...oltre che Moodle ormai presente da anni nella Scuola Secondaria, di cui è stato ampiamente implementato l'utilizzo. Inoltre, per curare l'aspetto psicologico degli alunni e la relazione docente discente, sono state attivate piattaforme per le video lezioni come Zoom e Jitsi Meet, Meet...Dal mese di Maggio, i docenti hanno utilizzato e continueranno ad utilizzare Teams di Office 365; da settembre tutto il personale scolastico e gli alunni si serviranno di Teams per le videolezioni. La scuola sta provvedendo alla profilazione di tutti gli alunni.

Per la Legge l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione. Tutti gli studenti sono tenuti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio –

non autorizzate, ed eliminare da Internet eventuali riferimenti offensivi o comunque illeciti (e inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.

Allo stesso tempo, gli allievi e i genitori devono fare un uso prudente dei Social Network, in particolare Facebook e Whatsapp, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre un'assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

3.9 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.

È inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

Tutti i servizi offerti tramite il sito web della scuola, nel rispetto delle norme vigenti, non potranno ricondursi ad esempio, anche indirettamente, al trattamento dei dati personali sensibili oppure a dati giudiziari.

3.10 Strumentazione personale: gestione degli strumenti personali – cellulari, tablet ecc.

"La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace".

BYOD letteralmente significa "porta il tuo dispositivo" ed è un'espressione che descrive quelle politiche aziendali che in tutto il mondo consentono agli impiegati di utilizzare i propri dispositivi personali in ambiente di lavoro.

In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici: si pensi, a titolo di esempio, agli student response systems ossia alla possibilità degli studenti e delle studentesse di rispondere a quiz e sondaggi utilizzando direttamente il proprio smartphone come telecomando sempre sotto la guida e il controllo dell'insegnante.

3.10.1 Per gli studenti

Considerato il cambiamento della didattica degli ultimi mesi, l'utilizzo dei dispositivi personali è consentito su indicazione del Docente che condivide con i propri studenti materiali didattici, elaborati digitali, file di diverso tipo: pdf, ppt, link a video, audio, tracce musicali...che consentano agli alunni non solo l'accesso e la visione ma la collaborazione e la modifica per il raggiungimento degli obiettivi programmati e delle competenze richieste.

L'uso della telefonia mobile e di strumenti informatici di proprietà dello studente, durante l'attività didattica, è consentita esclusivamente su richiesta del docente per scopi didattici, come ad esempio ricerche o consultazione di files precedentemente condivisi o elaborati sia dal docente che dagli alunni. È, inoltre, vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà e non, dello studente. L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzata dal docente.

3.10.2 Per i docenti

Durante le ore delle lezioni è consentito l'utilizzo del cellulare e di altri dispositivi elettronici personali solo a scopo didattico e integrativo di quelli scolastici disponibili, come ad esempio la compilazione del Registro Elettronico (presenze, assenze, ritardi, uscite anticipate, trascrizione compiti e attività giornaliera).

Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, a integrazione di quelli scolastici disponibili.

3.10.3 Per il personale della scuola

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

4. PREVENZIONE E RILEVAZIONE

La scuola è una comunità di dialogo, di ricerca, di esperienza sociale, basata su valori democratici e volta alla crescita della persona in tutte le sue dimensioni. Nella scuola ognuno, con pari dignità, seppur nella diversità di ruoli assunti, 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 nostro Istituto ha scelto una politica interna pro-attiva, tesa a creare un ambiente di apprendimento sereno e sicuro, che insegni a interagire in maniera responsabile. Nell'Istituto appare subito chiaro che cyberbullismo (e bullismo), prepotenza, aggressione e violenza non sono permessi; si incoraggiano gli studenti a parlare di sé e dei propri problemi; si stimola la partecipazione di tutta la comunità scolastica alle azioni finalizzate al contrasto del cyberbullismo (e bullismo).

Contrastare il cyberbullismo (e 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.

Per questo, in un'ottica di prevenzione, l'Istituto creerà, per il prossimo triennio, un insieme di attività, azioni e interventi che promuovano le competenze digitali ed evitino l'insorgenza di rischi legati proprio all'utilizzo del digitale, riducendo, quindi, le minacce per la sicurezza degli studenti di ogni ordine. Anche la letteratura di settore, infatti, dimostra come le migliori strategie di intervento siano quelle di carattere preventivo.

L'Istituto seguirà la strutturazione del concetto di prevenzione nei tre livelli stabiliti dall'Institute of Medicine, di seguito riportati:

- 1. Prevenzione Universale:** considerando tutti gli studenti potenzialmente a rischio, questo tipo di prevenzione prevede una serie di interventi diretti all'intera popolazione studentesca. Si tratta di interventi, quindi, ad ampio raggio. Tale prevenzione è estesa anche alla classe genitoriale.
- 2. Prevenzione Selettiva:** si tratta di azioni dirette a un gruppo di studenti in cui il rischio on line è stato individuato tramite precedenti indagini, segnalazioni fatte dalla scuola oppure dalla conoscenza della presenza di fattori di rischio presenti in quello specifico contesto e/o territorio. Gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving.
- 3. Prevenzione Indicata:** si tratta di interventi su un caso specifico, studiati per adattarsi agli studenti con l'obiettivo di ridurre i comportamenti problematici oppure dare supporto alle vittime. Questo tipo di intervento si avvale della professionalità di diverse figure perché spesso affronta problemi legati alla salute mentale del minore e, per questo, è opportuno coinvolgere anche la famiglia del/la ragazzo/a. In relazione alla Prevenzione Universale, la comunità scolastica sarà coinvolta in percorsi di prevenzione dei comportamenti a rischio e alle conseguenze relative all'assunzione di un comportamento a rischio, con specifico riferimento alle attività online. Tali percorsi avranno lo scopo di stabilire e condividere le regole scolastiche contro il cyberbullismo.

L'Istituto organizzerà eventi informativi e formativi diretti agli studenti in base alle diverse fasce d'età, come per esempio il progetto **“Generazioni Connesse”**, indirizzato alle classi V della Scuola Primaria, progetti in collaborazione con la Polizia di Stato e la Polizia Postale e delle Telecomunicazioni indirizzati alle classi quinte della Scuola Primaria e alle classi della Scuola Secondaria di Secondo Grado e/o progetti organizzati da associazioni ed enti territoriali.

Inoltre, il nostro Istituto, facendo parte della **“Rete delle Scuole di Aprilia contro il Bullismo”**, parteciperà anche agli eventi formativi e informativi organizzati dalla Rete rivolti ai genitori, ai ragazzi e a tutti gli operatori del settore.

Nelle azioni preventive ed educative, infatti, saranno chiamate in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma anche istituzioni e associazioni, ciascuna con un proprio compito nei confronti degli studenti. La necessità di questa collaborazione nasce dal riconoscimento, sia da parte dei genitori che da parte degli insegnanti, delle difficoltà a svolgere da soli la propria funzione formativa ed educativa.

In relazione alla Prevenzione Selettiva, che si terrà nelle classi, si potenzieranno le competenze emotive, sociali e relazionali degli studenti attraverso percorsi curriculari e di educazione socio-affettiva. Attraverso l'osservazione sistemica dei comportamenti a rischio si aiuteranno gli alunni coinvolti (vittime e/o carnefici) creando situazioni di dialogo che consentano di far emergere gli aspetti di criticità per i

quali, attraverso un confronto, si potrà intervenire, seguendo un percorso di rieducazione alla socialità. Inoltre, il coinvolgimento dei coetanei sarà indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto e sottrarre al "bullo" i potenziali gregari.

Relativamente alla Prevenzione Indicata, destinata ai singoli alunni che manifestano comportamenti a rischio di cyberbullismo (e/o bullismo), si attiverà un percorso di counseling con il supporto di personale specializzato che possa condurre l'alunno a riflettere sulle regole e sul loro rispetto, a definire i limiti del comportamento anti-sociale, a riconoscere i propri punti di forza, per ri-acquisire un certo livello di autostima. In questo contesto verranno condivise anche le sanzioni previste nel caso di comportamenti a rischio.

4.1.1 Rischi

I principali rischi legati a un utilizzo non consapevole del digitale e della Rete si riferiscono alla possibilità, da parte del minore, di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere le azioni dannose.

È necessario conoscere questi fenomeni per distinguerli tra loro in modo da poter adottare le strategie migliori per arginarli e contenerli. E', altresì, necessario, conoscere le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano.

I rischi cui sono esposti i minori sono numerosi, e derivano essenzialmente da un uso scorretto delle Tecnologie dell'Informazione e della Comunicazione (TIC).

La professoressa Ersilia Menesini dell'Università di Firenze ha suddiviso e classificato i rischi cui i ragazzi vanno incontro, sintetizzandoli nella tabella che segue:

	Contenuto Ragazzo destinatario di produzioni di massa	Contatto Ragazzo come partecipante (attività iniziate da adulti)	Condotta Ragazzo è attore (sia come vittima che come attore)
Aggressivo	Violenza / contenuti cruenti	Molestie, stalking	cyberbullismo
Sessuale	Pornografia	Grooming, richieste sessuali	Molestare sessualmente Sexting
Valori	Razzismo/odio	Persuasione ideologica	Autolesionismo anoressia
Commerciale	Vendita e sfruttamento	Violazione della privacy/ abuso di dati personali	Scaricare Gioco d'azzardo

Gli allievi sono potenzialmente esposti a tutti i rischi descritti. La Scuola, quindi, deve prenderli in considerazione tutti.

Nel nostro contesto sociale, complesso e prevalentemente per un mondo adulto, le TIC sono ormai parte integrante anche della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione. Le agenzie educative non devono associare tali strumenti al concetto di categoria adatta ai giovani perchè

“competenti”, sentendosi esonerati dal proprio ruolo educativo e dalla responsabilità di promuovere presso i più giovani un uso consapevole e integrativo (non sostitutivo) delle tecnologie digitali.

I rischi online, infatti, rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte dei giovani: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling, Internet addiction, videogiochi online, esposizione a contenuti dannosi o inadeguati, etc.

Infatti, eludendo la sorveglianza degli insegnanti, attraverso gli smartphone, dotati di particolari applicazioni e di collegamento a Internet, oltre che parlare e scrivere messaggi con i genitori, gli alunni potrebbero scaricare e spedire foto personali o intime, proprie o altrui, video con contenuti indecenti o violenti, accedere a Internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi.

4.1.2 Azioni

Nel corso del triennio l'Istituto attiverà una politica di sensibilizzazione sul tema, per accrescere la consapevolezza tra i giovani studenti dei problemi che potrebbero presentarsi all'interno di un gruppo relazionale. Le azioni che verranno intraprese saranno volte a incoraggiare gli studenti a modificare i propri comportamenti rendendoli più funzionali e a facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare su un obiettivo comune. Infine, l'Istituto favorirà la diffusione di informazioni e servizi rendendoli disponibili all'intera comunità scolastica.

In questa ottica, l'Istituto si occuperà di:

- intraprendere un'attività di peer education;
- proporre a tutte le classi V della Scuola Primaria attività inerenti al progetto “Generazioni connesse”;
- proporre a tutte le classi della Scuola Secondaria di Primo Grado progetti per la diffusione di un uso consapevole delle TIC e della Rete;
- istituire delle campagne di sensibilizzazione per mettere in luce i rischi di un utilizzo poco corretto delle TIC;
- promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR;
- elaborare una proposta 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 la sviluppo di un sistema di regole e di una cultura anti prepotenze nella classe;
- implementare l'e-Safety Policy con il contributo di tutte le componenti (docenti, studenti, famiglie, personale ATA).
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva presentando questa e-Safety Policy agli Organi Collegiali e quindi inserirla nel sistema di regolamenti della Scuola e renderla pubblica sul sito della Scuola.

4.2 Rilevazione

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle TIC, in cui il carnefice, in una posizione di forza rispetto alla vittima, assume atteggiamenti prevaricatori, secondo la logica dell'“asimmetria di potere”.

Il potere online deriva semplicemente dal possesso di specifiche competenze digitali o dal possesso di alcuni contenuti (come immagini, video o confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

I tratti specifici del cyberbullismo sono correlati all'impatto che le TIC hanno nella vita dei giovani e alle caratteristiche stesse della Rete, che non sempre mettono i ragazzi nella condizione di reale consapevolezza delle conseguenze delle proprie azioni.

Il cyberbullismo non è una problematica relativa unicamente a vittima e cyberbullo, ma è un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per i ragazzi come, appunto, la famiglia, la scuola, i media, le TIC e il gruppo dei pari.

Si riportano di seguito alcune considerazioni relative all'uso delle TIC e della Rete in generale, che determinano l'utilizzo delle tecnologie per compiere atti di cyberbullismo.

Impatto: la diffusione di materiale tramite la Rete è incontrollabile e senza limiti. Un contenuto offensivo e denigratorio online può, infatti, diventare virale e compromettere la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o città, anche se questo spesso non è sufficiente: la rete è ovunque.

Convinzione dell'anonimato: chi agisce online si sente protetto dall'anonimato, rimanendo nascosto dietro un nickname o cercando di non essere identificabile. In questa condizione ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. In realtà, l'anonimato è un “falso mito della Rete”: qualunque nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo è anche uno dei fattori alla base del forte stress percepito dalla vittima, che molte volte non può dare né un nome e né un volto al proprio aggressore.

Assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegner il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna a un senso costante di rabbia e impotenza.

Assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.

Indebolimento dell'empatia: esistono alcune cellule, chiamate neuroni specchio, che ci mettono in relazione con gli altri quando li abbiamo di fronte, permettendoci di capirli e di provare emozioni simili a quelle che loro provano, proprio come se fossimo di fronte a uno specchio. Quando le interazioni avvengono online, mancando la presenza fisica dell'altro che è sostituito dal dispositivo, la funzione speciale di questi neuroni viene meno. La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

Feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e questo riduce fortemente l'empatia e il riconoscimento del danno provocato.

Attraverso l'osservazione sistemica, è possibile rilevare alcuni segnali generali che la vittima di cyberbullismo può manifestare:

- appare nervosa quando riceve un messaggio o una notifica;
- sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- cambia comportamento e atteggiamento in modo repentino;
- mostra ritrosia nel dare informazioni su ciò che fa online;
- soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- inizia a utilizzare sempre meno computer e telefono;
- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- il suo rendimento peggiora.

Lo studente vittima di cyberbullismo può mostrare segni di tristezza, ansia o risentimento nei confronti di compagni o altre persone, riferendo spontaneamente, o su richiesta, l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola, e, grazie al confronto periodico con gli insegnanti, questi possono essere allertati e attivare misure di intervento.

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. Mentre il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno si deve rivolgere al genitore.

I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola dai minori (l'eventuale 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 rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, ecc.

5. SEGNALAZIONE E GESTIONE DEI CASI

5.1 Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'e-Policy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono

valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3 dell'e-Policy).

Nelle procedure sono indicate:

- le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola. Tali procedure sono comunicate e condivise con l'intera comunità scolastica. Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito Internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il

gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Si suggeriscono, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

5.2 Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

5.2.1 Strumenti a disposizione di studenti/esse

Studenti/esse per segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, possono utilizzare il seguente indirizzo e-mail dell'IC Matteotti, specifico per le segnalazioni:

sosmatteotti@gmail.com

oppure rivolgersi:

- allo sportello di ascolto con professionisti presente all'interno dell'I.C. stesso;
- al referente per il bullismo e ad altri docenti designati nei vari plessi.
- alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

5.3 Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

Helpline di Telefono Azzurro tel. 19696 è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

Co.Re.Com. (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

Via Lucrezio Caro, 67 00193 - Roma - tel. 06/3215995 - info@corecomlazio.it
www.corecomlazio.it/

Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

Viale Giorgio Ribotta, 41 - 00144 Roma - tel. 06. 77391 - direzione-lazio@istruzione.it -
www.usrlazio.it/

Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

Viale Trastevere, 191 00153 - Roma 06 588831 - tel. 06 5813429 - 06 5813608 -

poltel.rm@poliziadistato.it www.commissariatodips.it/

Piazzale dei bonificatori 8 04100 - Latina - tel. 0773 449210/14/20/24 - fax 0773449219 -
sez.polposta.it@pecps.poliziadistato.it

Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

Distretto Territoriale Latina c/o Poliambulatorio piazza Celli - Latina - tel. 0773 6556022 -
urp.distretto2@ausl.latina.it

Distretto Aprilia Via Giustiniano, 2H, 04011 Aprilia (Latina) tel: [06 928 6341](tel:069286341)

Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; raccolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

c/o Consiglio Regionale del Lazio Via della Pisana, 1301 00163 - Roma tel.06 6593 7314 - 4
falvaro@regione.lazio.it -
www.garanteinfanzia.regione.lazio.it

Sportello di Ascolto Istituzionale - Provincia di Latina: lo sportello è rivolto ai Minori e alle Famiglie del territorio provinciale.

c/o Provincia di Latina - Via Costa, 1 - 04100 LATINA Tel. 0773.401224
msansoni@regione.lazio.it

Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

**Via dei Bresciani, 32 – 00186 - Roma - tel.06. 688931 - tribmin.roma@giustizia.it
www.giustizia.it - TM di Roma**

Comitato Unicef Latina: su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

3477845325 - 327 8377432 - e-mail: comitato.latina@unicef.it

Centro Famiglia e Vita Consultorio diocesano Via Trieste 19, 04011 Aprilia (Latina)

tel. 06 9275185

Youpol: app realizzata dalla Polizia di Stato per segnalare episodi di spaccio, bullismo, reati di violenza che si consumano tra le mura domestiche. L'applicativo si può scaricare gratuitamente ed è disponibile per dispositivi [ios](#) e [Android](#).

5.4 Allegati con procedure schede di segnalazione e diario di bordo



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.
- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.
- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.

A) Se c'è fattispecie di reato - segue le procedure della scuola

B) Se non c'è fattispecie di reato

- Richiedi la consulenza dello psicologo/a scolastico

- Informa i genitori (o chi eserce la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condivide informazioni e strategie.

- Informa i genitori di ragazzi/e infra quattordicenni 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)

- Attiva il consiglio di classe.

- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).



© All rights reserved Generazioni Connesse 2019



Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori). Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

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 il consiglio di classe.
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Se emergono evidenze passa allo schema successivo

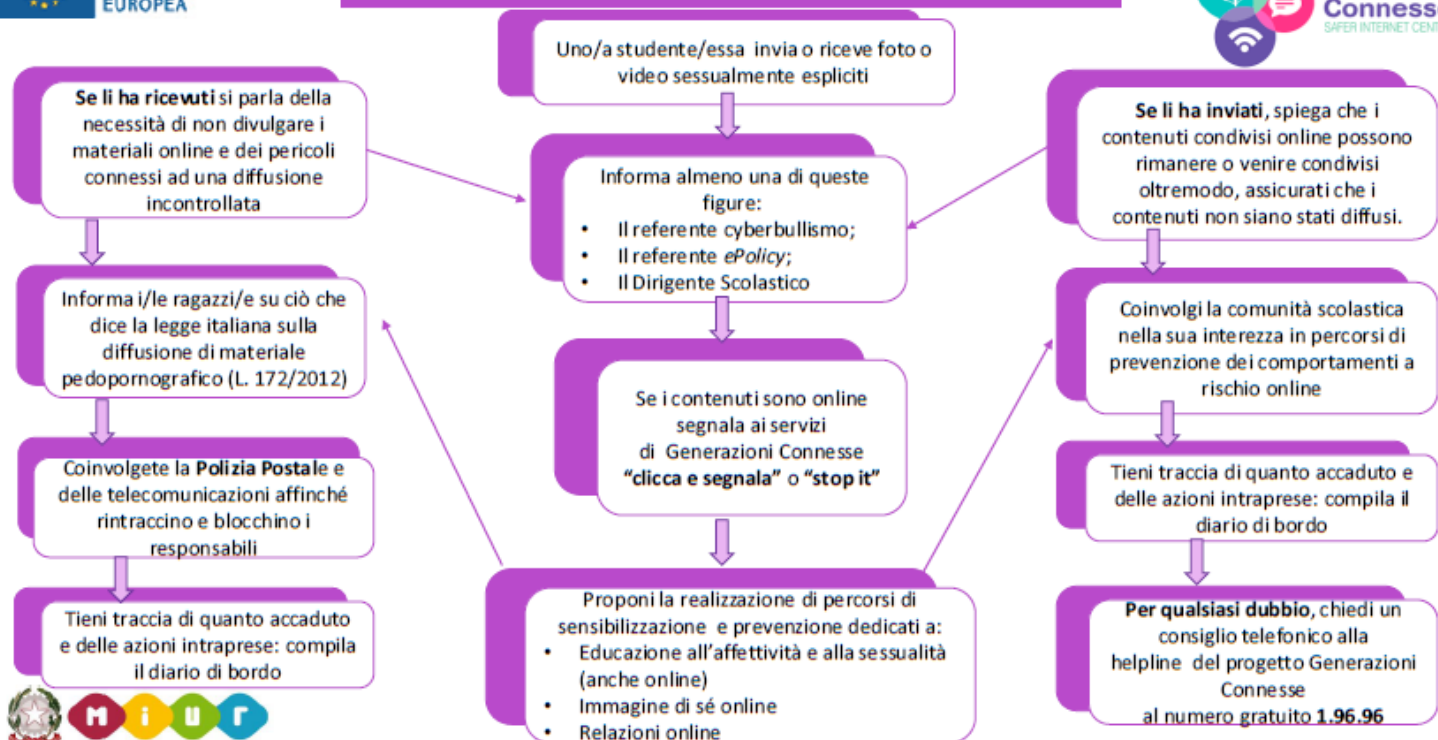
Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat



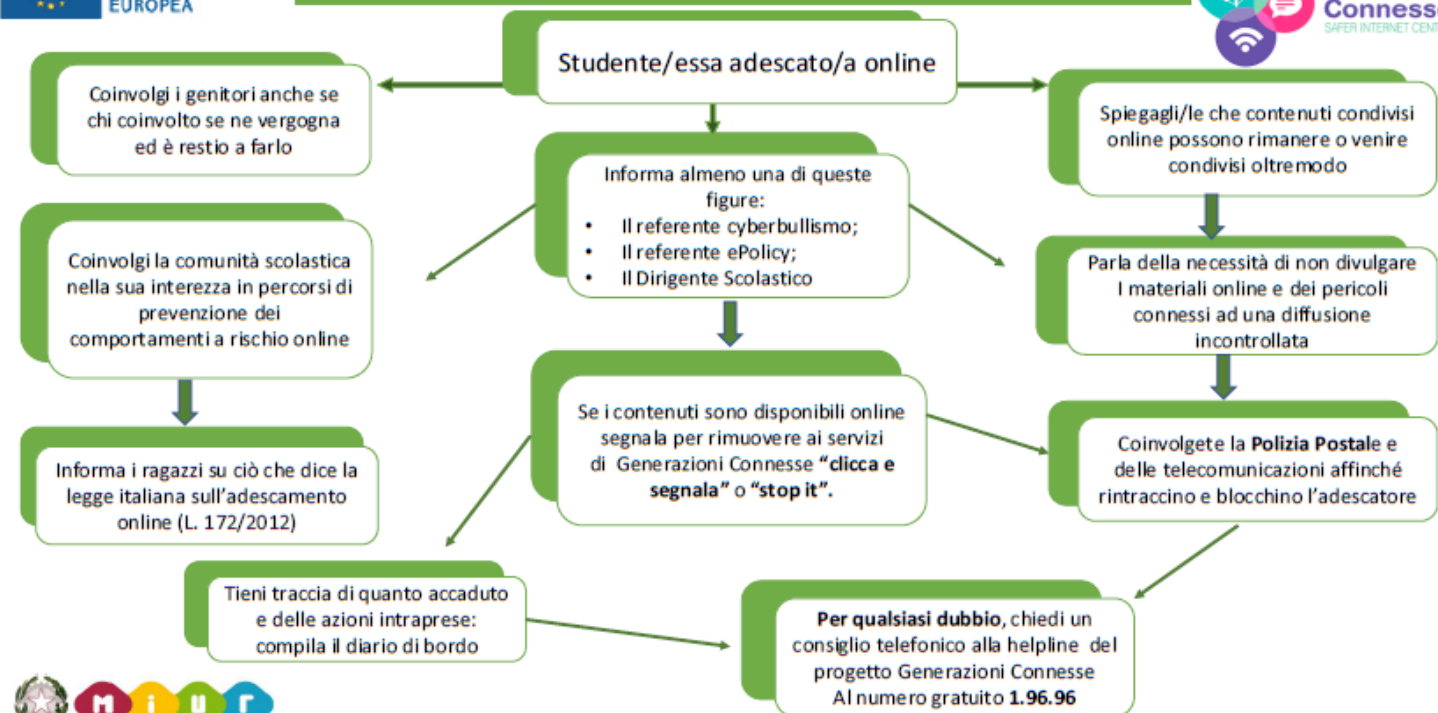
© All rights reserved Generazioni Connesse 2019

Procedure interne: cosa fare in caso di Sexting?

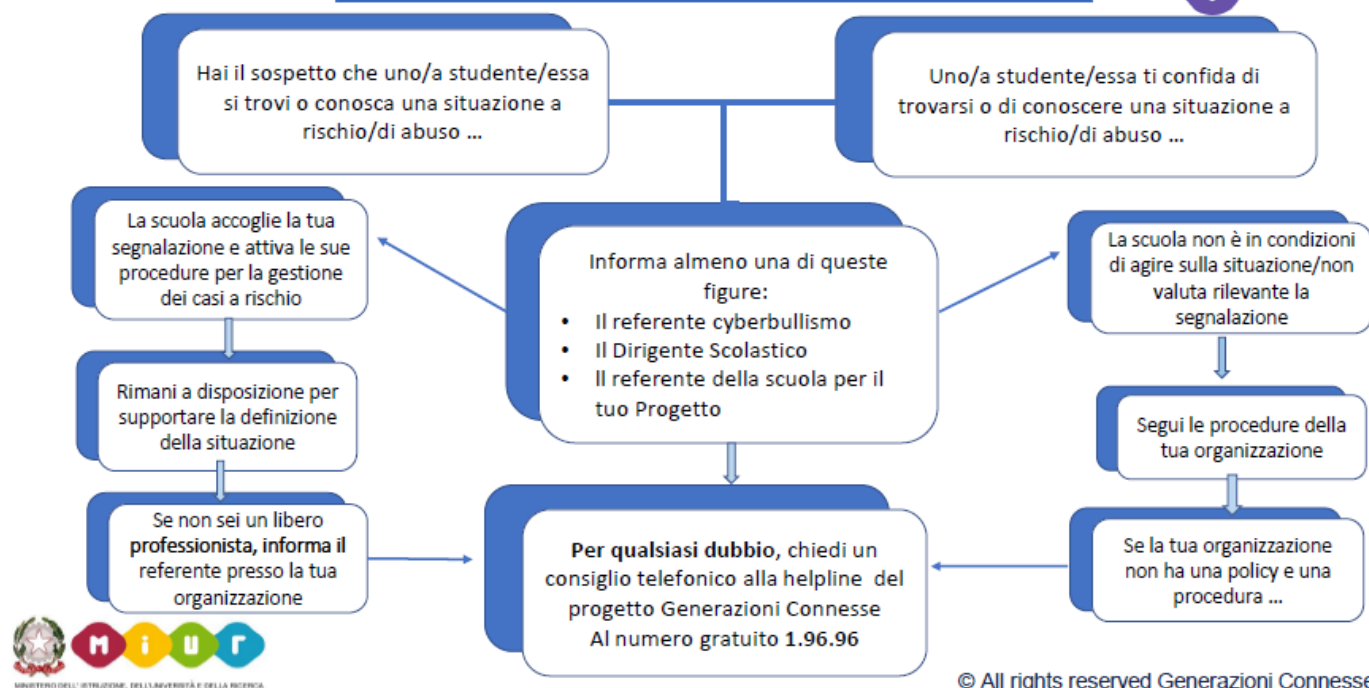


© All rights reserved Generazioni Connesse 2019

Procedure interne: cosa fare in caso di Adescamento Online?



© All rights reserved Generazioni Connesse 2019



© All rights reserved Generazioni Connesse 2019

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi							
Scuola _____				Anno Scolastico _____			
N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1..... Classe: 2..... Classe: 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: 2..... Classe: 3..... Classe:
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo?		
La famiglia o altri adulti hanno cercato di intervenire?		
Chi è stato informato della situazione?	☐ coordinatore di classe data: ☐ consiglio di classe data: ☐ dirigente scolastico data: ☐ la famiglia della vittima/e data:	☐ la famiglia del bullo/i data: ☐ le forze dell'ordine data: ☐ altro, specificare:

MODULO PER IL FOLLOW UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 2		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 3		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 4		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 5		☐ migliorata ☐ invariata ☐ peggiorata Come:

ANNESSI

1.LINEE GUIDA PER UNA SCUOLA LIBERA DA CYBERBULLISMO

1.1 LINEE GUIDA PER I RAGAZZI

Consigli per difendersi dai rischi legati all'uso delle nuove tecnologie

Il (cyber)bullismo è il termine che indica atti di bullismo e di molestia effettuati tramite e-mail, sms, blog, social network e Internet.

La forma on-line del bullismo ha alcune caratteristiche che la rendono particolarmente pericolosa perché:

1. il (cyber)bullismo è pervasivo: il cyberbullo può raggiungere la vittima in qualsiasi luogo e in qualsiasi momento;
2. è un fenomeno persistente: il materiale diffamatorio può rimanere disponibile per molto tempo;
3. spettatori e cyberbulli sono potenzialmente infiniti;
4. i protagonisti sono diversi: il cyberbullo può essere anche una persona estranea, può agire singolarmente o in gruppo e può, se vuole, rimanere anonimo o protetto da un avatar o da un nickname. Tutti quelli che osservano senza far nulla diventano corresponsabili delle azioni del cyberbullo; mettere un "like" su un social o condividere o commentare foto o video sottopone chi lo fa a una responsabilità maggiore.

1.2 LINEE GUIDA PER I GENITORI

Molti bambini utilizzano Internet già durante i primi anni della scuola primaria (6-7 anni). È importante sottolineare che è fondamentale l'accompagnamento all'utilizzo di Internet da parte di un adulto (genitore, insegnante, educatore) in relazione all'età del bambino.

I bambini al di sotto dei 10 anni, in genere, non avendo ancora sviluppato le capacità di pensiero critico necessarie, non sono in grado di esplorare il web da soli.

Con la preadolescenza e l'adolescenza s'intensifica l'uso di Internet: i giovani scaricano musica, utilizzano motori di ricerca per trovare informazioni, visitano siti, inviano e ricevono sms, la posta elettronica e i giochi online. La supervisione degli adulti è quindi fondamentale anche in questa fase, poiché una maggior conoscenza e consapevolezza legate alla crescita non mettono comunque al riparo dai rischi della Rete.

Come prevenzione è utile le impostazioni di filtri di navigazione che inibiscono la visita di alcuni siti web specifici, ma resta fondamentale il dialogo costante e continuo, la vicinanza e la partecipazione alle problematiche dei propri figli.

1.3 LINEE GUIDA PER LA SCUOLA

È proprio nel mondo della scuola che il bullismo, il più delle volte, si genera e si manifesta: il bullo attua le sue prepotenze e la vittima vive il suo dramma, facendo sì che l'esperienza scolastica acquisisca una connotazione negativa che va a influire sul normale sviluppo dei soggetti coinvolti.

I giovani, siano essi bulli o vittime, difficilmente parlano o si sfogano con gli adulti di quello che succede loro, gli uni per non essere scoperti e gli altri per paura di peggiorare la loro situazione.

Ecco perché la scuola rappresenta il luogo migliore in cui poter iniziare a fare prevenzione e in cui promuovere sia una cultura pro-sociale che veda, nell'altro diverso da sé, solo un altro modo di essere, né migliore, né peggiore, sia una cultura del confronto e del dialogo aperto, dove apprendere che il bullismo è un comportamento sbagliato e che solo parlandone lo si può riconoscere e sconfiggere.

La scuola, così come i genitori, ha il compito di guidare il ragazzo ad acquisire competenza e quindi anche una buona sicurezza, valorizzandolo e apprezzando le sue qualità personali positive.

2. DISPOSIZIONI A TUTELA DEI MINORI PER LA PREVENZIONE E IL CONTRASTO DEL FENOMENO DEL CYBERBULLISMO

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 proposta, già approvata dal Senato e poi modificata dalla Camera (20 settembre 2016), era stata nuovamente approvata con modificazioni dal Senato.

Il provvedimento introduce una serie di misure di carattere educativo e formativo, finalizzate in particolare a favorire una maggior consapevolezza tra i giovani del disvalore di 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 cyberbullismo in tutte le sue manifestazioni attraverso una strategia che comprende misure di carattere preventivo e 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 cyberbullismo 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 cyberbullismo 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 che dovrà collaborare con le Forze di polizia, e con le associazioni e con i centri di aggregazione giovanile presenti sul territorio;

- prevede interventi di caratteri educativo in materia di cyberbullismo (finanziamento di progetti e promozione dell'uso consapevole di Internet);
- in caso di episodi di cyberbullismo in ambito scolastico, prevede inoltre l'obbligo da parte del dirigente responsabile dell'istituto 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.

http://www.camera.it/leg17/522?tema=prevenzione_e_repressione_del_bullismo_e_del_cyberbullismo