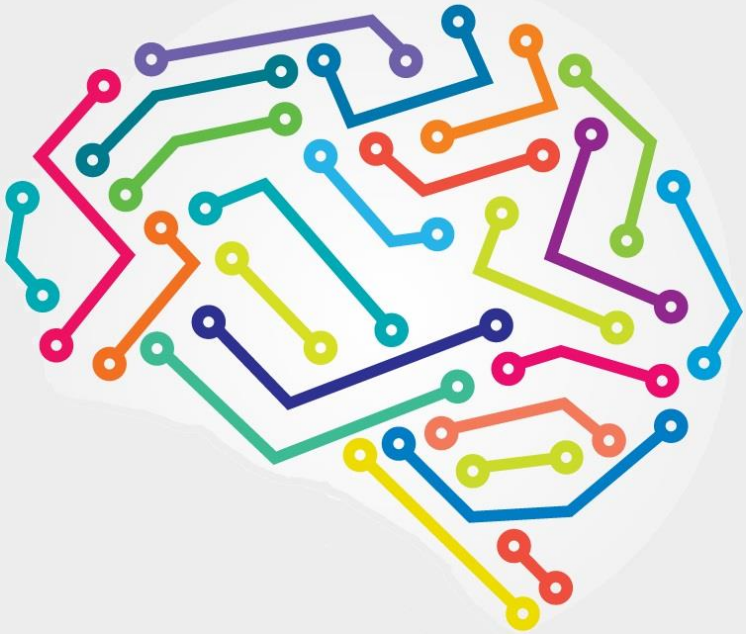


E - Policy

ISTITUTO COMPRENSIVO DI MEDESANO

DIGITAL-BRAIN

"Designed by Patrickss / Freepik"

Argomenti del Documento

1 Presentazione dell'E-policy

1.1 Introduzione ……... 1
1.2 Scopo dell'E-policy ……... 1
1.3 Ruoli e responsabilità ……... 2
1.4 Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto ……... 4
1.5 Condivisione e comunicazione dell'E-policy all'intera comunità scolastica ……... 4
1.6 Gestione delle infrazioni alla E-policy ……... 5
1.7 Integrazione dell'E-policy con regolamenti esistenti ……... 8
1.8 Monitoraggio dell'implementazione dell'E-policy e suo aggiornamento ……... 8

2 Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti ……... 9
2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica ……... 10
2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali ……... 10
2.4 Sensibilizzazione delle famiglie e Patto di corresponsabilità ……... 10

3 Gestione dell'infrastruttura e della strumentazione TIC (Tecnologie dell'Informazione e della Comunicazione) della e nella scuola

3.1 Protezione dei dati personali ……... 12
3.2 Accesso ad Internet ……... 12
3.3 Strumenti di comunicazione on-line ……... 12
3.4 Strumentazione personale ……... 14

4 Rischi on-line: conoscere, prevenire e rilevare

4.1 Sensibilizzazione e prevenzione ……... 15
4.2 Cyberbullismo: che cos'è e come prevenirlo ……... 15
4.3 Hate speech: che cos'è e come prevenirlo ……... 17
4.4 Dipendenza da Internet e gioco on-line ……... 17
4.5 Sexting……... 18
4.6 Adescamento on-line ……... 18
4.7 Pedopornografia ……... 19

5 Segnalazione e gestione dei casi

5.1 Cosa segnalare……... 21
5.2 Come segnalare: quali strumenti e a chi ……... 22
5.3 Gli attori sul territorio per intervenire……... 23
5.4 Allegati con le procedure ……... 24
5.5 Regolamento BYOD ……... 31

1 Presentazione dell'E-policy

1.1 Introduzione

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.
Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).
In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte degli alunni che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.
L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali.
Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza on-line e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione sui comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

1.2 Scopo dell'E-policy

Perché è importante dotarsi di una E-policy?
L'E-policy è lo strumento operativo al quale tutta la comunità educante dovrà fare riferimento, al fine di:

- assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace,
- sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L'E-policy ha lo scopo di:

- fornire delle linee guida per garantire il benessere in rete,
- definire regole di utilizzo delle TIC a scuola,
- porre le basi per azioni formative ed educative su e con le tecnologie digitali,
- sensibilizzare su un uso consapevole delle stesse.

L'E-policy è un documento programmatico volto a promuovere:

- le competenze digitali,
- un uso delle tecnologie digitali positivo, critico e consapevole,
- l'acquisizione di abilità e competenze sia da parte degli alunni che degli adulti coinvolti nel processo formativo.

L'Istituto Comprensivo di Medesano ha elaborato questo documento in conformità con le "Linee di orientamento per azioni di contrasto al bullismo e al cyberbullismo" del 15 aprile 2015 e successiva nota Miur di aggiornamento "Linee di orientamento per la prevenzione del bullismo e del cyberbullismo" dell'ottobre 2017, con l'obiettivo di educare e sensibilizzare gli alunni, gli insegnanti, i genitori e l'intera comunità educante, all'uso sicuro e consapevole di Internet.
Infatti lo sviluppo delle nuove tecnologie, il loro utilizzo nell'ambito didattico e la maggiore diffusione

nella vita di tutti i giorni di questi strumenti richiede maggiore responsabilità e consapevolezza.
È compito dell'intera comunità scolastica, genitori inclusi, garantire che gli alunni siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro. Di qui la necessità di dotare la Scuola di una propria Policy di E-safety, per gestire anche le eventuali infrazioni come integrazione del Regolamento d'Istituto.

1.3 Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante, è necessario che ognuno, secondo il proprio ruolo, si impegni nell'attuazione e nella promozione di essa.
La nostra scuola, nel farsi carico della formazione globale dell'individuo nella fase evolutiva che va dai 3 ai 14 anni, deve individuare in maniera chiara e inequivocabile ruoli e responsabilità di ciascuno degli attori del percorso formativo nella promozione dell'uso consapevole della rete.

Il Dirigente Scolastico:

- organizza e/o favorisce l'adesione del personale della scuola ad una corretta formazione sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete;
- organizza e/o favorisce l'adesione del personale docente ad una formazione adeguata relativa all'uso delle TIC nella didattica;
- garantisce che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantisce l'organizzazione di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- garantisce che la scuola utilizzi un Internet Service filtrato approvato e conforme ai requisiti di legge;
- segue le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;
- è parte integrante del protocollo da seguire in caso di infrazione della E-policy.

L'Animatore digitale, supportato dal Team dell'innovazione:

- stimola la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce consulenza e informazioni al personale anche in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola, nonché propone la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili;
- assicura che gli utenti possano accedere alla rete Wi-Fi della scuola tramite password applicate e regolarmente cambiate e cura la progettazione dello sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- diffonde la E-policy attraverso materiali multimediali appositamente creati e/o attraverso corsi specifici.

Il Referente del bullismo e cyberbullismo:

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo (può avvalersi della collaborazione delle Forze di polizia, Associazioni e centri di aggregazione giovanile del territorio);
- coinvolge (ove possibile), con progetti e percorsi formativi ad hoc, alunni, colleghi e genitori.

Il Direttore dei servizi generali e amministrativi:

- assicura, 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;
- garantisce il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, etc.) 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.

I Docenti:
- si informano/aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantiscono che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi, nella misura e nei tempi più idonei per il gruppo a cui ci si rivolge;
- garantiscono che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- assicurano 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;
- garantiscono 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;
- assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- riuniti in team e Consigli di Classe, stabiliscono le linee guida da adottare relativamente all'utilizzo degli strumenti digitali in classe durante l'orario scolastico; tutti gli insegnanti che lavorano sul gruppo in esame saranno tenuti a rispettare le linee condivise;
- controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, etc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni a siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicano 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;
- segnalano qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalano al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

Il Personale scolastico:
- comprende e contribuisce a promuovere politiche di e-sicurezza;
- è consapevole dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;
- monitora l'uso di dispositivi tecnologici e attua le politiche scolastiche in relazione all'utilizzo delle TIC;
- segnala qualunque abuso sospetto o problema ai docenti coordinatori delle classi di appartenenza degli alunni coinvolti;
- usa comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;
- garantisce che le comunicazioni digitali con gli alunni siano gestite attraverso sistemi scolastici ufficiali.

Gli Alunni:

- sono responsabili, in relazione al proprio grado di maturità e di apprendimento, dell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- hanno 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;
- comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottano condotte rispettose degli altri anche quando si comunica in rete;
- esprimono domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori.

I Genitori:

- sostengono la linea di condotta che la scuola adotta nei confronti dell'utilizzo delle TIC nella didattica;
- seguono gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la rete e comunicano con loro circa i problemi rilevati quando i figli non usano responsabilmente le tecnologie digitali o Internet;
- fissano delle regole per l'utilizzo del computer e tengono sotto controllo l'uso che i figli fanno di Internet e dello smartphone in generale;
- accettano e condividono quanto scritto nell'E-policy dell'Istituto.

Infine, gli Enti esterni e le Associazioni:

- si conformano alla politica della scuola riguardo l'uso consapevole delle TIC e della rete;
- promuovono comportamenti sicuri, la sicurezza on-line e assicurano la protezione degli alunni durante le attività che si svolgono insieme.

1.4 Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli alunni. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social).
L'Istituto, all'atto della sottoscrizione del contratto con il personale esterno, qualora si tratti di specialisti che avranno bisogno delle TIC, fornisce informativa riportante le principali regole da seguire in materia ed il Regolamento relativo con esplicitati i modi e le procedure di segnalazione delle infrazioni in materia. Coloro che entreranno a lavorare nell'Istituto dovranno accettare e condividere il documento di E-policy che sarà consultabile sul sito della Scuola.

1.5 Condivisione e comunicazione dell'E-policy all'intera comunità scolastica

Il documento di E-policy verrà adottato dal Collegio dei Docenti e approvato dal Consiglio di Istituto. Automaticamente l'approvazione da parte dei due organi modificherà ed integrerà il Regolamento d'Istituto vigente.

1.6 Gestione delle infrazioni alla E-policy

Qualora si abbia il sospetto o un ragionevole dubbio rispetto ad una eventuale infrazione di uso o di gestione delle TIC; il personale interno ed esterno, gli alunni, le famiglie ed il personale, avranno come primo riferimento all'interno dell'Istituto, il docente presente in classe o il docente coordinatore di classe.
Le possibili problematiche possono essere sostanzialmente di due tipi:
1) problemi legati alla strumentazione,
2) problemi legati all'uso off-line e on-line della strumentazione.

1) *problemi legati alla strumentazione*

I Plessi dell'IC di MEDESANO dispongono complessivamente di laboratori informatici, LIM, stampanti e vari devices fissi o portatili ad esclusivo uso didattico. Alunni, docenti, educatori e personale ATA possono utilizzarli a condizione di avere cura dei componenti hardware e software di tali strumenti. Le apparecchiature presenti nella Scuola sono un patrimonio comune, quindi vanno utilizzate con il massimo rispetto e minimizzando gli sprechi di risorse (energia, carta, inchiostro, etc.).
Gli insegnanti sono responsabili degli strumenti che stanno utilizzando e hanno il compito di responsabilizzare anche gli alunni, per renderli consapevoli dell'importanza della salvaguardia di un bene comune. In caso di danno che non risulti evidentemente accidentale, il responsabile sarà tenuto a risponderne.
Salvo esplicita autorizzazione del Referente informatico del plesso, non è consentito:

- modificare il sistema operativo o le sue impostazioni generali;
- installare e disinstallare i programmi o modificarne le impostazioni (ivi incluse le estensioni dei browser);
- scaricare o caricare software non legato alle finalità didattiche;
- utilizzare software di condivisione come Torrent, P2P, emule, etc.;
- modificare le impostazioni per l'accesso alla rete o installare modem o altri dispositivi per l'accesso indipendente ad Internet;
- utilizzare le stampanti, CD, DVD o altro a fini personali;
- copiare, caricare o scaricare musica, film, programmi e qualsiasi altro materiale non legato alla didattica o vincolato da copyright o comunque in conflitto con le norme dei codici civile e penale riguardanti il diritto d'autore, la privacy, la divulgazione di materiale offensivo, pedo-pornografico etc.

In caso di problemi di qualsiasi natura legati agli strumenti informatici, si dovrà intervenire rispettando la seguente sequenza di responsabilità:
A. il docente che sta utilizzando lo strumento è il primo che può identificare il problema e cercare di risolverlo;
B. se non è in grado, si rivolgerà al Referente informatico del plesso;
C. se neanche lui dovesse riuscire, si contatterà il docente tecnico dell'Istituto o il tecnico esterno a cui è affidata la manutenzione dei laboratori.

2) *problemi legati all'uso off-line e on-line della strumentazione*

In caso di uso scorretto dei devices, sia in fase di "sospetto" che in caso di "certezza" relativi a situazioni presenti o passate, il docente coordinatore di classe sarà informato immediatamente e allerterà il team docente della classe o delle classi che potrebbero essere coinvolte e al contempo invierà una E-mail preliminare al Dirigente.
Nel momento in cui fosse comprovata l'infrazione e che la suddetta necessiti di intervento specifico, il team docente si riunisce e verbalizza la riunione. Si cercherà una strategia di intervento che risulti educativamente formativa.
Qualora il team docente lo ritenesse opportuno, il coordinatore contatterà la famiglia dei coinvolti spiegando loro la situazione ed informandola dei passi che si intendono intraprendere.

Le azioni che si intraprenderanno partiranno dal ritiro del device con avviso alla famiglia per il ritiro a scuola della stessa; un periodo di sospensione, adeguato rispetto all'azione intrapresa, dall'utilizzo dei devices a scuola; nei casi più gravi si potranno anche comminare sospensioni con obbligo di frequenza.
A seconda della tipologia dell'infrazione si potrebbe anche ritenere opportuno l'accesso delle famiglie e degli alunni coinvolti allo sportello psicologico dell'Istituto.
Il Dirigente Scolastico e i singoli docenti che usano le TIC e che si accorgono di comportamenti scorretti hanno il diritto di revocare l'accessibilità in modo temporaneo o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (tablet, notebook, account di Google etc.).

Il nostro Istituto ha redatto anche un
REGOLAMENTO DI DISCIPLINA PER LA SCUOLA SECONDARIA DI PRIMO GRADO
La scuola è luogo di formazione della persona e di educazione mediante lo studio. Persegue obiettivi culturali ed educativi finalizzati all'evoluzione delle conoscenze e all'inserimento nella vita attiva.
La scuola è una comunità di dialogo, di ricerca, di esperienza sociale, ispirata ai valori democratici e alla crescita della persona in tutte le sue dimensioni. Fonda il suo progetto e la sua azione educativa sulla qualità della relazione insegnante-alunno.
La vita della comunità scolastica si basa sulla libertà d'espressione, di pensiero e di religione, sul rispetto reciproco di tutte le persone che la compongono.
Il seguente Regolamento di disciplina individua i comportamenti che configurano mancanze disciplinari con riferimento ai doveri elencati nello "Statuto delle studentesse e degli studenti della Scuola secondaria", le relative sanzioni e gli organi competenti ad irrogarle.

Il procedimento rispetterà i seguenti criteri:

- Ogni provvedimento disciplinare deve avere finalità educative.
- Le sanzioni devono essere proporzionate all'infrazione disciplinare e ispirate al principio della riparazione del danno.
- La responsabilità disciplinare è personale.
- Nessuna infrazione disciplinare connessa al comportamento può influire sulla valutazione del profitto.
- L'alunno deve sempre potere esprimere le proprie ragioni.
- Nel caso della sanzione della sospensione dalle lezioni fino a 15 gg, un genitore, in rappresentanza dell'alunno, sarà preventivamente udito dal Consiglio di Classe. La mancata presentazione dell'alunno o del genitore comporta la rinuncia al diritto di difesa.
- Nel caso della sanzione della sospensione dalle lezioni superiore a 15 gg, un genitore, in rappresentanza dell'alunno, sarà preventivamente udito dal Consiglio d'Istituto. La mancata presentazione del genitore comporta la rinuncia al diritto di difesa.
- La sanzione della nota sul registro viene irrogata dal docente che constata l'infrazione, o sulla base di rapporto di altro operatore scolastico che l'ha constatata.
- Ogni provvedimento di sospensione dalla scuola da 1 a 15 gg. disposto nei casi previsti dal presente regolamento è sempre adottato dal Consiglio di Classe.
- Ogni provvedimento di sospensione dalla scuola superiore ai 15 gg., disposto nei casi ritenuti più gravi, è sempre adottato dal Consiglio di Istituto.
- Le sanzioni previste dal presente regolamento saranno proporzionate e graduate dagli organi competenti, sulla base del caso in esame, nel rispetto delle normative vigenti.
- Le sanzioni irrogate e notificate sono immediatamente esecutive ai sensi dell'art. 21 quater della L.241/1990.

ORGANO DI GARANZIA INTERNO
E' istituito apposito ORGANO DI GARANZIA, interno alla scuola, composto dal Dirigente Scolastico, due docenti, due genitori e due membri supplenti, designati dal Consiglio d'Istituto a cui è ammesso ricorso da parte dei genitori, in merito all'erogazione delle sanzioni disciplinari del presente regolamento.

- L'Organo di Garanzia resta in carica tre anni.

- L'Organo di garanzia si riunisce ogni volta che è chiamato a decidere sulle sanzioni irrogate dagli organi competenti della scuola.
- L'Organo di Garanzia decide sui ricorsi per l'abrogazione delle sanzioni disciplinari irrogate secondo il presente regolamento e formula proposte al Consiglio d'Istituto per la modifica del regolamento stesso.
- Per le sanzioni che prevedono la sospensione dalle lezioni, entro 15 giorni dalla data di notifica del provvedimento, è possibile fare ricorso davanti all'Organo di Garanzia che dovrà deliberare in merito entro 10 giorni.
- Le decisioni dell'Organo di Garanzia vengono prese a maggioranza. In caso di parità nel voto la sanzione non è applicabile e decade. L'astensione equivale a voto contrario. Le sedute sono regolarmente verbalizzate.
- Le decisioni assunte vengono emanate per iscritto e notificate alle persone interessate con atto scritto del Dirigente Scolastico, il quale emana il decreto di revoca ovvero di conferma del provvedimento, in attuazione della delibera dell'organo di garanzia.
- L'Organo di Garanzia viene anche interpellato, su richiesta dei genitori, o di chiunque vi abbia interesse, anche sui conflitti che sorgono all'interno delle scuole in merito all'applicazione del presente Regolamento. Il parere reso dall'organo di garanzia è comunicato alle persone interessate dal Dirigente Scolastico.

Il presente Regolamento costituisce parte integrante del Regolamento di Istituto.
Copia del presente Regolamento è pubblicata sul sito Istituzionale della scuola, dandone avviso ad alunni e genitori.
Si riporta solo la parte relativa al rispetto sulle norme della privacy, al rispetto della normativa sull'uso dei cellulari e al rispetto della normativa riguardante gli atti di cyberbullismo L 71/2017.

DOVERI	COMPORTAMENTI	PROVVEDIMENTI E SANZIONI
Rispetto delle norme sulla privacy	L'alunno acquisisce immagini, suoni, filmati riconducibili a persone e/o ambienti scolastici mediante telefoni cellulari e altri dispositivi elettronici e successivamente li divulga tramite mms e/o via Web, ivi comprese la pubblicazione su siti Internet e/o social network.	1. Richiamo del docente con nota sul diario e sul registro elettronico, convocazione dei genitori alla presenza del Dirigente Scolastico; 2. Ritiro immediato del telefono (se sorpreso in flagrante) e restituzione solo ai genitori; 3. Sospensione con durata di uno o più giorni a discrezione del consiglio di classe; 4. Segnalazione all'autorità competente.
Rispetto della normativa sull'uso dei telefoni cellulari	L'alunno viene colto ad utilizzare il cellulare in qualsiasi ambiente scolastico o il cellulare lasciato acceso suona a scuola.	1. Richiamo del docente con nota sul diario e sul registro elettronico; 2. Ritiro immediato del telefono; 3. Restituzione del telefono solo ai genitori.
Rispetto della normativa riguardante gli atti di cyberbullismo L. 71/2017	Uso di linguaggio volgare, violento, offensivo o diffamatorio in ambienti virtuali, durante l'orario scolastico ed extrascolastico. Comportamenti o linguaggi minacciosi, discriminatori e/o lesivi dei diritti, della dignità e della sensibilità delle persone, esercitati nei locali della scuola oppure fuori da questa, anche attraverso i social network. (Si precisa che tali comportamenti hanno un forte impatto sulle dinamiche relazionali tra alunni e quindi anche sulla vita scolastica).	1. Nota sul diario e sul registro elettronico da parte del docente che ne viene a conoscenza, previo adeguato accertamento. Convocazione dei genitori da parte del Dirigente Scolastico. Sospensione con durata di uno o più giorni, a discrezione del consiglio di classe; 2. Segnalazione all'autorità competente. Ammonimento del Questore per alunni di età superiore ai 14 anni*.

*Si precisa che nel caso di reiterate violazioni al presente Regolamento di disciplina, agli alunni non sarà consentita la partecipazione alle visite d'istruzione (V. Regolamento d'Istituto – Allegato 3 – art.9)

1.7 Integrazione dell'E-policy con regolamenti esistenti

Una volta approvato il documento di E-policy dal Collegio dei Docenti e dal Consiglio di Istituto, lo stesso andrà ad integrazione dei regolamenti vigenti.

1.8 Monitoraggio dell'implementazione dell'E-policy e suo aggiornamento

All'inizio di ogni anno scolastico l'Animatore Digitale, riguarderà il documento di E-policy e apporterà eventualmente le necessarie modifiche. Ogni modifica sostanziale verrà portata in Collegio e in Consiglio per l'approvazione.

AZIONI

- A 1 anno
  - Realizzazione di un sistema di monitoraggio delle attività (azione sviluppabile nell'arco di un anno)
  - Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti, anche all'interno del Collegio dei docenti.
  - Prevedere attività specifiche in vista della giornata mondiale contro il cyberbullismo (visione di video, manufatti, diffusione del materiale reperito sul sito di Generazioni Connesse, letture di libri, incontri con l'autore, drammatizzazioni delle letture, etc.).

- A 3 anni
  - Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli alunni di Scuola secondaria di primo grado.
  - Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori della Scuola secondaria di primo grado.
  - Prevedere incontri tra la polizia postale e gli alunni della Scuola secondaria di primo grado durante l'anno scolastico.

2 Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Il nostro Istituto negli ultimi anni si è fortemente impegnato nella attuazione del PNSD (*"Piano Nazionale Scuola Digitale"*), aderendo ai bandi PON, investendo in infrastrutture, sperimentando nuove metodologie didattiche e impegnandosi in un percorso continuo di formazione del personale docente ed amministrativo.
Per permettere la realizzazione di questa nuova didattica, viene messo a disposizione degli alunni e di tutto il personale quanto serve per accedere a Internet, lavorare, comunicare e collaborare avvalendosi delle nuove tecnologie.
Il curricolo scolastico dell'Istituto prevede il regolare utilizzo nei laboratori e nelle aule di devices con cui alunni e insegnanti svolgono attività di produzione, ricerca e scambio di materiale.
I ragazzi usano la rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "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 ("Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli alunni verso un uso consapevole e responsabile delle tecnologie digitali.
Ciò avviene attraverso la progettazione e implementazione di un curricolo digitale che è stato integrato nel curricolo didattico ed è consultabile nel curricolo allegato al PTOF d'Istituto.
In relazione alla E-policy il curricolo si impegna, nel rispetto delle età dei discenti, a favorire negli alunni lo sviluppo delle seguenti competenze e comportamenti:

- sviluppare una serie di strategie atte a permettere di valutare l'attendibilità delle informazioni reperite in rete;
- avere la consapevolezza dell'esistenza "di un punto di vista" che "guida" i fornitori di informazioni on-line;
- sapere come affinare una ricerca;
- sapere che scaricare file musicali o video in modo fraudolento è un reato;
- sapere come relazionarsi e interagire in un ambiente condiviso on-line avendo particolare cura nel preservare i propri dati sensibili;
- capire che, manipolando fotografie e falsando la propria identità reale in ambienti condivisi, si possono attirare attenzioni "sbagliate";
- capire che gli amici on-line potrebbero non essere chi dicono di essere;
- capire il motivo per cui non si dovrebbero condividere resoconti dettagliati delle proprie vite o informazioni sensibili;
- comprendere il motivo per cui non si debbano pubblicare foto o video di terzi senza il loro permesso;
- sapere cosa siano: cyberbullismo, sexting e grooming;
- sapere a chi rivolgersi per chiedere aiuto in caso di problemi legati all'uso di Internet.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo. Ciò si rende necessario per fornire agli alunni modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.
In particolare il nostro Istituto prevede di:

- implementare le reti;
- svolgere costanti attività di ricognizione e messa a punto delle dotazioni digitali;
- proporre e comunicare iniziative interne di formazione costruite in base alle richieste dei docenti stessi;
- fornire l'informazione di corsi di formazione/aggiornamento di Ambito 13 o di altra natura tramite invio di E-mail da parte della segreteria e/o dell'Animatore digitale;
- favorire la diffusione di pratiche e strumenti attraverso la creazione di E-mail esplicative, piccoli tutorial o incontri formativi nei quali ci si scambiano informazioni;
- informare e formare tutto il nuovo personale con indicazioni sulla E-safety Policy d'Istituto.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi on-line.
Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione:

- del personale specializzato interno (Animatore digitale, Referente bullismo e cyberbullismo);
- se necessario del personale esterno (professionisti qualificati);
- con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc.), delle Amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti sul territorio.

2.4 Sensibilizzazione delle famiglie e Patto di corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità.
Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme gli alunni verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura.
L'Istituto garantisce:

- corretta e puntuale informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali previste dall'E-policy;
- l'aggiornamento del Regolamento scolastico,
- l'aggiornamento del "Patto di corresponsabilità";
- la creazione di una sezione dedicata sul sito web dell'Istituto;
- puntuale informazione rispetto al fatto che l'utilizzo di Internet è monitorato.

AZIONI

- A 1 anno
    - Organizzazione di un Regolamento informatico di Istituto.
    - Creare una rete di supporto per i docenti per agevolare tutti nell'uso delle TIC a scuola

sia per la DDI che per la DaD.
    - Creare materiali illustrativi dematerializzati che riprendano gli aspetti principali dell'uso sicuro e consapevole di Internet e delle tecnologie digitali.
    - Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

- A 3 anni
    - Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
    - Organizzare incontri per i docenti sulle competenze digitali.
    - Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

3 Gestione dell'infrastruttura e della strumentazione TIC (Tecnologie dell'Informazione e della Comunicazione) della e nella scuola

Il nostro Istituto è dotato di LIM con accesso ad Internet in tutte le classi; inoltre, presso la Scuola secondaria di primo grado, si trova anche un laboratorio con postazioni collegate in rete e dotate di accesso ad Internet appositamente filtrato.

3.1 Protezione dei dati personali

La maggior parte dei dati sensibili viene gestita dagli uffici di segreteria che hanno una rete intranet dedicata ed opportunamente protetta.
I docenti gestiscono i dati personali degli alunni o attraverso devices dotati di password e forniti dalla scuola o utilizzando strumenti personali sempre dotati di password d'accesso.
I dati personali dei docenti vengono tutelati e gestiti esclusivamente dalla segreteria e solo per scopi Istituzionali. Le comunicazioni vengono normalmente gestite tramite il registro elettronico in uso; diversamente si utilizza l'indirizzo E-mail istituzionale @icmedesano.edu.it.

3.2 Accesso ad Internet

In ogni plesso è possibile connettersi ad Internet mediante cavo di rete o via Wi-Fi. Tutti i computer e tablet della scuola sono già impostati per accedere direttamente alla rete; il personale scolastico può accedere con devices privati richiedendo le credenziali di accesso e impegnandosi a non perderle e a non divulgarle. Agli alunni è consentito l'accesso alla rete Wi-Fi solo per fini didattici e sotto il controllo del docente.

3.3 Strumenti di comunicazione on-line

La nostra Scuola ha differenti strumenti di comunicazione on-line:
1) E-mail

Il nostro Istituto ha attivato il dominio scuola.edu.it associato alla piattaforma di Google "G-suite for Education". Tutto il personale ottiene ogni anno un account [nome.cognome@icmedesano.edu.it] con cui accedere e lavorare in ambiente Google a titolo gratuito e in modo protetto, utilizzando i servizi di posta elettronica, archivio on-line, creazione di documenti e numerose altre applicazioni. La stessa opportunità è offerta agli educatori e ai rappresentanti dei genitori che ne facciano richiesta e a tutti gli alunni, previa accettazione da parte delle famiglie delle regole di utilizzo di tale servizio e firma di una liberatoria, nell'ottica della indispensabile condivisione di responsabilità rispetto all'utilizzo dell'account che verrà attivato per i loro figli.
L'attivazione di tale servizio per gli alunni comporta necessariamente la consapevole accettazione di quanto segue:

- la posta elettronica e tutte le applicazioni abilitate devono essere utilizzate esclusivamente per svolgere attività didattiche secondo le indicazioni della Dirigenza, del Collegio dei docenti o del docente responsabile della lezione;
- per nessuna ragione è consentito scaricare o caricare nulla a fini personali (file musicali, foto, software, video, etc.), tranne nel caso di specifiche attività didattiche preventivamente programmate e regolamentate dai docenti;
- l'Istituto prenderà tutte le precauzioni per garantire che gli alunni non abbiano accesso a materiale non adeguato, pur sapendo che è oggettivamente impossibile azzerare tale rischio; pertanto, si accetta come condizione necessaria al mantenimento della sicurezza interna all'Istituto che in qualsiasi momento i docenti amministratori possano accedere

all'account degli alunni per verificare, sospendere o eliminare l'account di coloro che facciano un uso improprio di questo servizio.

Tutto il personale scolastico deve tenere presente che:

- le credenziali di accesso (nome utente e password) sono strettamente personali ed ogni attività non regolare sarà imputata al titolare delle credenziali;
- l'utilizzo delle caselle di posta elettronica e del sistema cloud della scuola non è consentito per attività personali non attinenti la didattica o la propria attività istituzionale;
- è possibile iscriversi a siti, blog, forum o altro utilizzando l'account di Gsuite per finalità didattiche o istituzionali solo dopo aver interpellato l'amministrazione scolastica e l'aver verificato l'impatto di tale attività con il regolamento privacy;
- la riservatezza dei dati condivisi in Drive è responsabilità in primis del proprietario del file e, a seguire, di chi ha accesso al file in condivisione.

A tutela della privacy di tutti i nostri utenti, si fa presente che tutti i dati sono di proprietà esclusiva dell'Istituto e non di Google e il docente amministratore del servizio può gestire gli accessi alle applicazioni attribuendo agli utenti diversi livelli di autonomia a seconda dei ruoli e delle funzioni. Se si dovesse rendere necessario per fini di sicurezza interna, tutti gli account potranno essere sottoposti a verifica, sospesi o eliminati dall'amministratore del servizio. Amministratori del servizio sono il Dirigente Scolastico e un docente da lui incaricato. Al termine del percorso scolastisco, o in caso di trasferimento ad altra sede, gli account verranno sospesi o eliminati al 31 agosto con un preavviso di una settimana.

2) *Sito web della scuola*

Il sito della scuola è curato da responsabili incaricati dal Dirigente Scolastico che operano sotto il diretto controllo suo e, per quanto riguarda la parte amministrativa, del DSGA. I materiali che vengono pubblicati sul sito rappresentano l'istituzione scolastica e concorrono a determinarne l'immagine all'interno e all'esterno della scuola stessa; è pertanto necessario un controllo costante della loro legittimità nonché del loro valore comunicativo, formativo e culturale. Tale attività di controllo e selezione viene effettuata dal docente responsabile del sito, in collaborazione con il team digitale e il resto del collegio docenti, sotto la supervisione del Dirigente Scolastico. La scuola fornirà ai genitori una informativa con validità annuale che esprime le modalità relative alla pubblicazione di materiale prodotto dagli alunni; le fotografie o i filmati degli alunni in occasione di gite, visite d'istruzione, durante la didattica, saranno pubblicati sul sito della scuola, ai fini della documentazione e divulgazione dell'esperienza previa liberatoria firmata dai genitori in sede d'iscrizione (leggi 196/2003-305/2006 Codice materia protezione dati personali). In caso di inserimento di immagini di persone esterne alla scuola, la scuola fornirà un'informativa che esprime le modalità relative alla pubblicazione.

La scuola individuerà un gruppo, facente parte del personale scolastico, che si occuperà di inserire i contenuti sul sito istituzionale. I dipendenti saranno formati per queste mansioni. La password temporanea assegnata dovrà essere modificata dal dipendente al primo accesso e conservata con la massima cura. Le credenziali di accesso rimangono attive fino alla permanenza del dipendente in servizio nell'Istituto.

3) *Sicurezza rete Lan e Wireless – Wi-Fi*

I computer dell'amministrazione sono su una rete locale isolata dal resto della rete della Scuola secondaria di primo grado. Il collegamento di computer portatili o palmari personali alla rete di Istituto avviene attraverso Wi-Fi o Lan per mezzo di password fornita esclusivamente al personale della scuola e ad uso esclusivo. Tutti i dispositivi in dotazione vengono settati con password preimpostata in modo da non rendere necessaria la condivisione della stessa con gli alunni o esperti esterni.

La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati. La memorizzazione dei documenti e delle impostazioni personali è garantita attraverso il meccanismo di profilo mobili di Windows, che archivia centralmente sul server di dominio i dati e li rende disponibili in tutte

le postazioni legate alla didattica per quanto riguarda il laboratorio della Scuola secondaria di primo grado. Le postazioni singole nelle aule di tutti i plessi dell'Istituto non sono invece messe in rete. Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su un supporto personale (Pendrive, Hard Disk esterni, o altro) dei propri dati. Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione.
Gli alunni possono accedere alla rete Wi-Fi con supporti digitali personali grazie all'attivazione del BYOD (come declinato all'#6 PNSD).

3.4 Strumentazione personale

Gli alunni possono portare a scuola i propri devices personali (smartphone, tablet, notebook, …) a condizione di utilizzarli esclusivamente a fini didattici e previa autorizzazione esplicita da parte del docente; in assenza di quest'ultima, devono rimanere spenti e fuori dalla portata degli alunni. Sono esempi di possibile utilizzo consentito la consultazione di e-book e libri digitali o la produzione di foto e filmati di fasi di lavoro nel corso di attività di laboratorio. Non è consentito, sempre a titolo esemplificativo, utilizzare il cellulare per telefonare, fotografare o filmare compagni e docenti, navigare su Internet a fini personali e/o non consentiti. Nel caso di un uso non autorizzato o in qualunque modo non idoneo all'attività didattica di tali strumenti durante le ore di lezione, il docente è autorizzato a ritirarli e a contattare la famiglia dell'alunno per la riconsegna; nei casi più gravi, può essere convocato il Consiglio di Classe per valutare possibili sanzioni disciplinari.

CD, DVD, Pendrive e altri dispositivi di storage dei dati.
Si possono utilizzare solo per finalità strettamente connesse alla didattica, ferma restando la diretta ed esclusiva responsabilità del proprietario, sia per la natura dei dati salvati sia per il rischio di trasmissione o ricezione di virus o altri programmi malware. Agli alunni è consentito l'utilizzo solo dopo esplicita autorizzazione da parte del docente. La scuola non è responsabile della custodia di qualsiasi device personale e in caso di danni o smarrimento non effettua risarcimenti.
I docenti e il personale della scuola possono utilizzare cellulari e tablet, a scopo personale, non durante l'attività didattica o lavorativa.

AZIONI

- A 1 anno
  - Realizzazione di un sistema di monitoraggio delle attività (azione sviluppabile nell'arco di un anno)
  - Organizzare uno o più eventi o attività volti a formare gli alunni della Scuola secondaria di primo grado dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
  - Organizzare uno o più eventi o attività volti a formare gli alunni dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

- A 3 anni
  - Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
  - Organizzare materiali on-line volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
  - Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

4 Rischi on-line: conoscere, prevenire e rilevare

4.1 Sensibilizzazione e prevenzione

Il rischio on-line si configura come la possibilità per il minore di:

- commettere azioni on-line che possano danneggiare sé o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

Gli adulti della comunità educante hanno il dovere di mettere in campo tutte le strategie possibili al fine di contenere i rischi legati all' "abuso" di tecnologie.
Sostanzialmente le strade che possono essere intraprese sono due:

1) arginare le possibilità di incappare in qualche situazione a rischio;
2) dotare i ragazzi degli strumenti conoscitivi e valoriali tali da renderli in grado di discriminare le situazioni nelle quali si trovano coinvolti e, nel caso, di segnalare eventuali anomalie.

I due percorsi possibili sono, evidentemente, complementari e vanno correttamente bilanciati anche in relazione all'età dell'alunno.
Si può benissimo ritenere che, in effetti, si tratti di un unico percorso che differenzia al suo interno le percentuali dei due aspetti a seconda della situazione in cui ci si trova. E' altresì importante avere ben chiaro che un aspetto senza l'altro renderà il processo di crescita sempre e comunque incompleto.
Gli adulti della comunità educante hanno il "dovere" di vigilare, ma hanno soprattutto il compito di fornire agli alunni gli strumenti più idonei con i quali affrontare le situazioni cogliendone gli aspetti rischiosi e avendo una rete di sostegno attorno così chiara e solida da impedire loro cadute troppo rovinose.
Parlando della *sensibilizzazione* facciamo riferimento a tutte quelle azioni che si pongono come obiettivo quello di fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
Quando invece facciamo riferimento alla *prevenzione* ci riferiamo a quell'insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali; questo permetterà di ridurre i rischi legati all'utilizzo del digitale.
Il nostro Istituto Comprensivo, consapevole dei rischi insiti nell'uso del digitale, inserisce i concetti e le pratiche di sensibilizzazione e prevenzione nella didattica e, in caso di particolari iniziative, attiva un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, ASL,etc.), al fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano on-line.
Cercheremo di percorrere nei paragrafi successivi quali siano i principali pericoli on-line a cui si espongono i ragazzi che navigano.

4.2 Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il *cyberbullismo*:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative Linee di orientamento per la prevenzione e il contrasto del cyberbullismo indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo.

Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio Referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli alunni (ed ex alunni) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- azioni preventive ed educative e non solo sanzionatorie;
- nomina del Referente per le iniziative di prevenzione e contrasto che ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo.

A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio. Potrà svolgere un importante compito di supporto al Dirigente Scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), atti e documenti (PTOF, PdM, Rav).

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti ripetuti nel tempo.
Quando queste vessazioni vengono fatte on-line, diventano cyberbullismo.
Il cyberbullismo presenta le seguenti caratteristiche:

- è invasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- è un fenomeno persistente: il materiale messo on-line vi può rimanere per molto tempo;
- ha una platea potenzialmente infinita: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

A seconda dei casi, si potranno adottare azioni di prevenzione universale, selettiva e indicata.

1) Prevenzione Universale

Un programma di questo tipo parte dal presupposto che tutti gli alunni siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale.
Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

2) Prevenzione Selettiva

Un programma dedicato ad un gruppo di alunni in cui il rischio on-line è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem-solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

3) Prevenzione Indicata

Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli alunni con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia dell'alunno.

4.3 Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo on-line) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, etc.) ai danni di una persona o di un gruppo.
Tale fenomeno, purtroppo, è sempre più diffuso ed è estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli alunni gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Al termine della sezione vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica. Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.
In tal senso occorre:

- valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo, etc.).

4.4 Dipendenza da Internet e gioco on-line

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della rete. L'Istituto è intenzionato a promuovere azioni di prevenzione ponendo l'attenzione sul benessere digitale. Tale dipendenza, che può manifestarsi anche attraverso le ore trascorse on-line a giocare, rappresenta una questione importante per la comunità scolastica, che deve attenzionare il fenomeno e fornire gli strumenti agli alunni affinché questi siano consapevoli dei rischi che comporta l'iperconnessione. L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie, per favorire il "benessere digitale", ossia la capacità di creare e mantenere una relazione sana con la tecnologia.
Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche on-line;
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio le notifiche).

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise. Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in rete.

4.5 Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i ragazzi e le ragazze lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perché facilmente modificabili, scaricabili e condivisibili, e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico. I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn", letteralmente "vendetta porno", fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione.

4.6 Adescamento on-line

Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla rete per entrare in contatto con loro. I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi on-line, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming on-line.
In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).
A termine della sezione vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento. La problematica dell'adescamento on-line (come quella del sexting) si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale. Al fine di prevenire casi di adescamento on-line è opportuno, pertanto, accompagnare gli alunni in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.
È importante, inoltre, che gli alunni sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa.
Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.
Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità on-line, la capacità di gestire adeguatamente le proprie relazioni on-line (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).
Se si sospetta o si ha la certezza di un caso di adescamento on-line è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore.
È importante che il computer o altri dispositivi elettronici del minore-vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento on-line richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video, etc.).
L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, etc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

4.7 Pedopornografia

La pedopornografia on-line è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.
La legge n. 269 del 3 agosto 1998 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella legge n. 38 del 6 febbraio 2006 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori.
Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.
Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali. In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.
Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali" (Hotline). Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete.
I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.
Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc. Se si è a

conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on-line. Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale on-line rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale on-line si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale.

AZIONI

- A 1 anno
    - Realizzazione di un sistema di monitoraggio delle attività (azione sviluppabile nell'arco di un anno)
    - Organizzare uno o più incontri di sensibilizzazione sui rischi on-line e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli alunni della Scuola secondaria di primo grado.

- A 3 anni
    - Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli alunni, con il coinvolgimento di esperti.
    - Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
    - Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica (con le TIC) e assicurando la partecipazione attiva degli alunni.

5 Segnalazione e gestione dei casi

5.1 Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che un alunno possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento on-line ha a disposizione le procedure definite qui di seguito 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 on-line a rischio degli alunni (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione on-line 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 gli alunni in difficoltà.
Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.
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 secondaria di primo grado individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola e 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 agli alunni, 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:

- l'invio di E-mail contenente il documento di E-policy al personale scolastico e alle famiglie;
- una sezione dedicata nel sito della scuola;
- i collegi docenti e
- tutti i canali maggiormente utili ad un'efficace comunicazione.

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

1) Cyberbullismo

E' 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 alunni coinvolti (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

2) Adescamento on-line

Se si sospetta un caso di adescamento on-line è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne; é inoltre 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.

3) 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 se on-line, per quanto possibile, e il blocco della sua diffusione via dispositivi mobili. Per quanto riguarda la necessità di segnalazione e rimozione di contenuti on-line lesivi, ciascun minore 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.

Vi suggeriamo, 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 on-line. I minori potrebbero riferire all'insegnante fatti o eventi personali o altrui, accaduti anche al di fuori della scuola, che potrebbero mettere in allarme il docente.

Pertanto sono da considerare degni di segnalazione:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà di eventi privati, etc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, etc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), etc.

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 alunni, 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:

1) caso A (sospetto)

Il docente ha il sospetto che stia avvenendo qualcosa tra gli alunni della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento on-line.

2) caso B (evidenza)

Il docente ha evidenza certa che stia accadendo qualcosa tra gli alunni della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento on-line.

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

Strumenti a disposizione degli alunni

Per aiutare gli alunni a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo E-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;

- sportello di ascolto con professionisti;
- docente Referente per le segnalazioni.

Inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96. Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura Referente per il cyberbullismo. La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (Allegato 2), alla Referente, la quale, insieme al team per le emergenze, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente Scolastico. Sarà poi il Dirigente Scolastico, insieme al team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio.

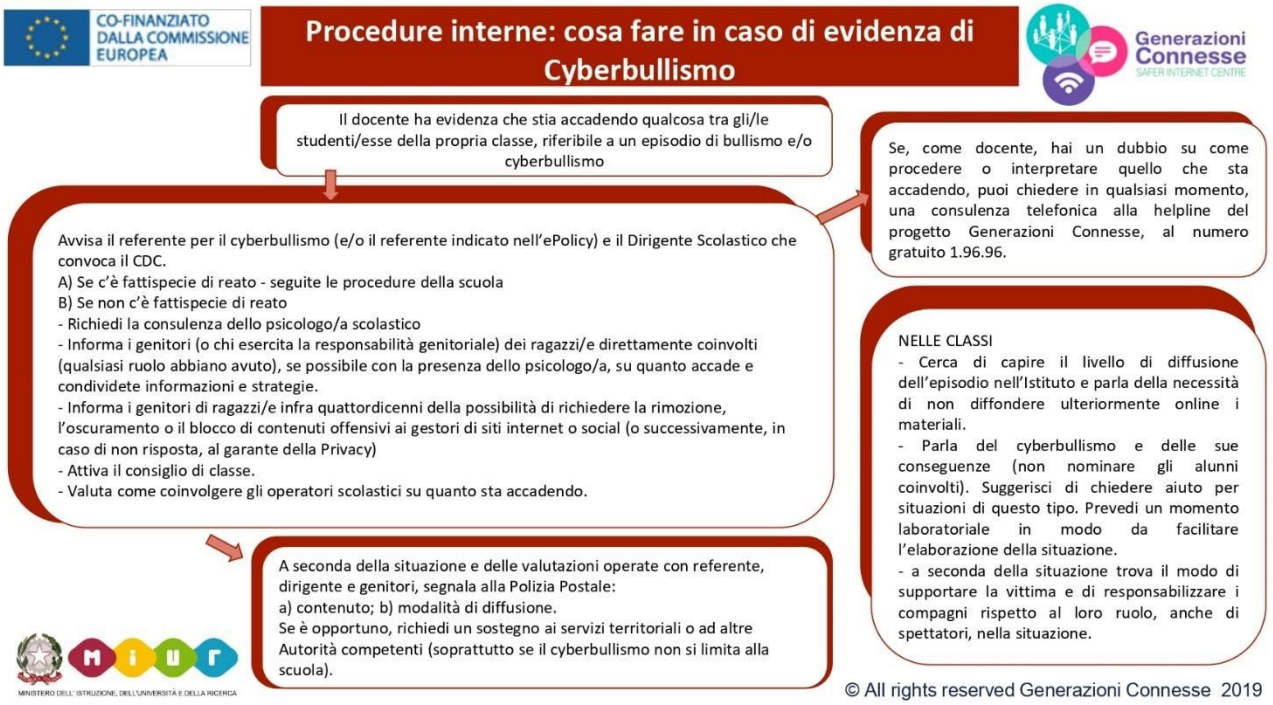
5.3 Gli attori sul territorio per intervenire

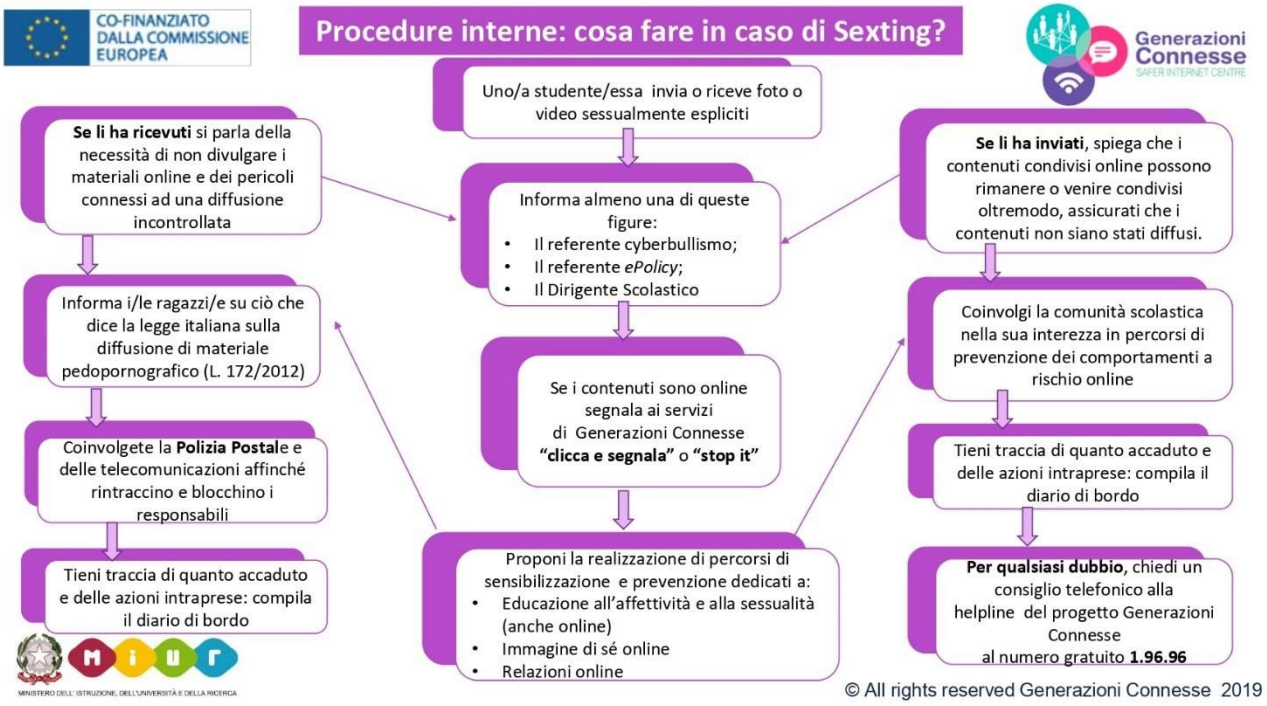
Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola. Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani"
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. Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
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.
Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
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.
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in rete.
Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono 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.
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.
Nei casi di maggiore gravità, si valuterà anche il coinvolgimento di attori esterni quali Forze dell'ordine e Servizi sociali. I documenti relativi alle procedure operative e i protocolli sono da elaborare in collaborazione con i suddetti attori del territorio, con cui siglarli unitamente.

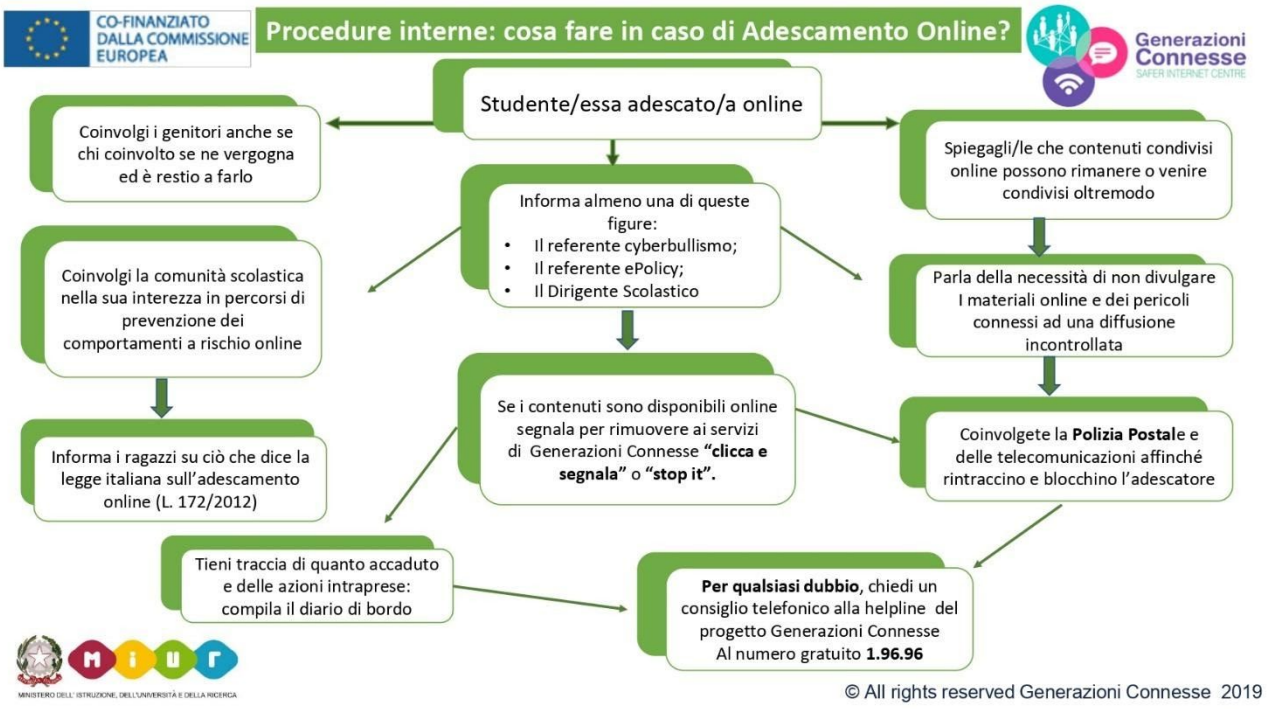
Il nostro piano d'azioni
Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli alunni in orario scolastico, vi sono le seguenti:

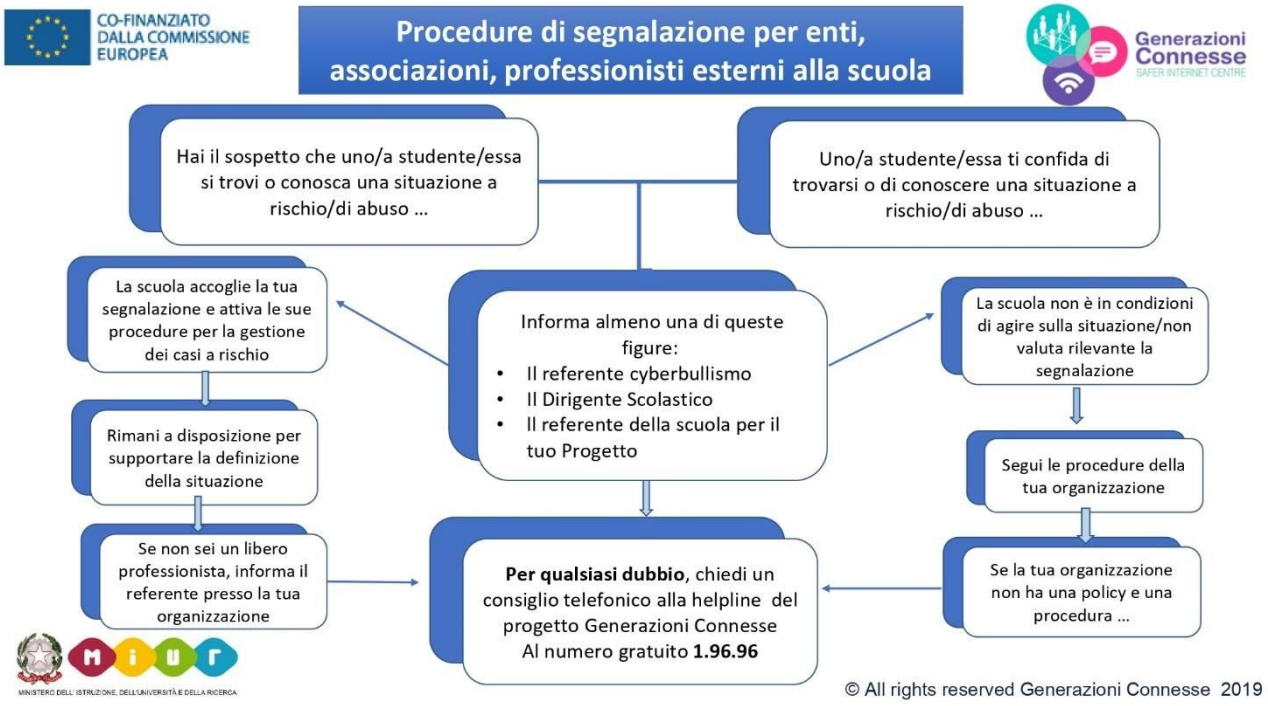
- diffondere un'informazione capillare rivolta al personale scolastico, agli alunni e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli alunni in orario scolastico se non per programmate attività didattiche.

5.4 Allegati con le procedure




CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di Sexting?
Generazioni Connesse
SAFER INTERNET CENTRE
Uno/a studente/essa invia o riceve foto o video sessualmente espliciti
Se li ha ricevuti si parla della necessità di non divulgare i materiali online e dei pericoli connessi ad una diffusione incontrollata
Informa almeno una di queste figure:
• Il referente cyberbullismo;
• Il referente ePolicy;
• Il Dirigente Scolastico
Se li ha inviati, spiega che i contenuti condivisi online possono rimanere o venire condivisi oltremodo, assicurati che i contenuti non siano stati diffusi.
Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012)
Se i contenuti sono online segnala ai servizi di Generazioni Connesse "clicca e segnala" o "stop it"
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino i responsabili
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Proponi la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
• Educazione all'affettività e alla sessualità (anche online)
• Immagine di sé online
• Relazioni online
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
MIUR
MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
SAFER INTERNET CENTRE
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Informa almeno una di queste figure:
• Il referente cyberbullismo;
• Il referente ePolicy;
• Il Dirigente Scolastico
Spiegagli/le che contenuti condivisi online possono rimanere o venire condivisi oltremodo
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Parla della necessità di non divulgare I materiali online e dei pericoli connessi ad una diffusione incontrollata
Se i contenuti sono disponibili online segnala per rimuovere ai servizi di Generazioni Connesse "clicca e segnala" o "stop it".
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
MIUR
MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse
SAFER INTERNET CENTRE
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Informa almeno una di queste figure:
• Il referente cyberbullismo
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Rimani a disposizione per supportare la definizione della situazione
Segui le procedure della tua organizzazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
Se la tua organizzazione non ha una policy e una procedura …
MIUR
MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019

Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

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

© All rights reserved Generazioni Connesse 2019

	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:

© All rights reserved Generazioni Connesse 2019

Altri documenti reperibili sulla piattaforma

https://www.generazioniconnesse.it

- Diario di bordo,
- iGloss@ 1.0 l'ABC dei comportamenti devianti on-line,
- Elenco dei reati procedibili d'ufficio.

Riferimenti per l'Emilia Romagna

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA Viale Aldo Moro, 50 40127 Bologna 051. 5276263 - 051. 5275713 garanteinfanzia@regione.emilia-romagna.it www.assemblea.emr.it/garanti/attivita-e-servizi/infanzia
Competenze/Servizi | Segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti a rischio: tutte
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti che configurano un reato: tutte Emilia Romagna

UFFICIO SCOLASTICO REGIONALE Via de' Castagnoli, 1 40126 - Bologna 051. 37851 direzione-emiliaromagna@istruzione.it www.istruzioneer.it/
Competenze/Servizi | Tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di Internet. Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti a rischio: cyberbullismo
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti che configurano un reato: cyberbullismo

TRIBUNALE PER I MINORENNI via del Pratello, 36 40122 – Bologna 051. 2964880 tribmin.bologna@giustizia.it http://www.tribmin.bologna.giustizia.it/
Competenze/Servizi | Tra le varie attività si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela e assistenza.
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti a rischio: ---
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti che configurano un reato: tutte

POLIZIA POSTALE E DELLE COMUNICAZIONI Via Francesco Zanardi, 28/6 - Bologna 051. 6352611 poltel.bo@poliziadistato.it www.commissariatodips.it/
Competenze/Servizi | Si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di Internet e che si configurano come reati.
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti a rischio: ---
Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti che configurano un reato: furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line (nel caso di clonazione di carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting 48

AZIENDE SANITARIE LOCALI I riferimenti per contattare le aziende sanitarie della propria città si trovano al seguente link: http://salute.regione.emilia-romagna.it/ssr/

aziende-sanitarie-irccs/erogazione-dellassistenza-aziende-sanitarieirccs-asp
Competenze/Servizi | Per avere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |
tipologie di comportamenti a rischio: tutte Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio | tipologie di comportamenti che configurano un reato: tutte

Istituto Comprensivo di Medesano

Via De Gasperi 2
43014 Medesano (PR)
C.M. PRIC80900A
C.F. 92103030349

tel 0525.420.403
fax 0525.422.659
mail pric80900a@istruzione.it
web www.icmedesano.edu.it

REGOLAMENTO BYOD

REGOLAMENTO PER L'UTILIZZO DEI DISPOSITIVI DIGITALI PERSONALI A SCUOLA

Premesse

A) La diffusione delle tecnologie informatiche in tutti i settori della società offre straordinarie opportunità ma presenta anche rischi, tali da consigliare alle scuole un approccio consapevole e ragionato a queste nuove tecnologie in ambito didattico.

B) Per tale ragione, in coerenza con quanto previsto dal Piano Nazionale Scuola Digitale (PNSD d'ora in avanti) il/la Istituto Scuola con indirizzo intende favorire l'uso consapevole e responsabile dei dispositivi digitali mobili, aprendosi alla loro integrazione nell'attività didattica quotidiana.

Articolo 1 – Definizione

Per BYOD, acronimo dell'inglese Bring Your Own Device (porta il tuo dispositivo), si intende un'innovativa politica educativa che in tutto il mondo consente agli studenti ed ai docenti di portare a scuola i propri dispositivi tecnologici e di utilizzarli per scopi didattici.

Articolo 2 – Dispositivi ammessi

Sono ammessi i seguenti dispositivi digitali mobili: tablet, PC portatili, e-reader e smartphone.

Articolo 3 – Autorizzazione all'uso didattico dei dispositivi

Gli alunni, fermo restando quanto previsto dal Regolamento d'Istituto, possono usare i propri dispositivi mobili per l'attività didattica nell'edificio scolastico e nelle sue pertinenze solo:

a) previa delibera del Consiglio d'Istituto precedente all'avvio dell'anno scolastico per le classi individuate;

b) previa delibera del Consiglio di Classe/interclasse, inserita nel piano di lavoro annuale e nel patto formativo, che consenta ai docenti interessati di sperimentare la modalità BYOD, anche solo in alcune discipline e/o in alcune specifiche situazioni.

c) c) con il consenso esplicito del docente in classe/interclasse.

Articolo 4 – Responsabilità individuale

Ogni studente è responsabile della custodia e del corretto utilizzo del proprio dispositivo: la scuola non sarà ritenuta responsabile dello smarrimento, furto o danneggiamento del bene.

Il dispositivo in nessun caso può essere lasciato a scuola oltre l'orario delle lezioni e incustodito durante lo svolgimento delle stesse.

Ogni alunno dovrà presentarsi a scuola, quando richiesto, con il proprio dispositivo, garantendone la funzionalità (adeguata capienza di memoria, carica, etc.) come qualsiasi altro supporto alla didattica. Si suggerisce di dotarsi eventualmente di caricabatteria portatile.

La dimenticanza del dispositivo o l'eventuale limitazione della sua funzionalità dovuta a negligenza dell'alunno saranno sanzionate a discrezione del docente.

Articolo 5 – Limitazioni d'uso

All'interno dell'Istituto il dispositivo e la sua connessione internet devono essere impiegati esclusivamente a fini didattici.

Non è consentito l'uso delle applicazioni di registrazione audio/video e della fotocamera non espressamente autorizzati dal docente in servizio e senza il consenso dei soggetti coinvolti.

Qualsiasi uso improprio ~~e~~ o non autorizzato potrà essere sanzionato dal punto di vista disciplinare mediante, a seconda della gravità dell'infrazione, il ritiro e la sospensione dell'uso del dispositivo stesso durante l'attività con eventuale ricaduta sulla valutazione della stessa.

Articolo 6 – Connessione alla rete Wi-Fi dell'Istituto

La connessione alla rete Wi-Fi d'Istituto da dispositivi mobili personali è vietata, salvo che sia stata autorizzata in via preventiva, temporaneamente o per l'intero anno scolastico, dal Dirigente Scolastico in considerazione di specifiche esigenze didattiche.

Articolo 7 – Condivisione di file

L'accesso eventuale alle cartelle d'Istituto sarà garantito prioritariamente alle classi per le quali il BYOD sia stato deliberato dal Consiglio di Istituto.

Per iscriversi a questo servizio sarà necessario creare un apposito indirizzo di posta elettronica, che dovrà ricalcare il modello seguente:
account@indirizzoscuola

Sarà cura di ciascun utente garantire la protezione del/dei dispositivo/i da virus, malware, spyware ed adware che potrebbero essere causa di perdita di dati e di potenziali minacce alla Sicurezza informatica di tutti gli altri utenti.

Articolo 8 – Tutela della riservatezza e dei diritti di proprietà intellettuale

Gli studenti devono rispettare la riservatezza, i diritti d'immagine, d'autore e di proprietà ~~e~~ intellettuale altrui.
Non è ammessa la copia, la duplicazione, la manomissione, il salvataggio su proprio o altrui dispositivo, l'alterazione, la diffusione di prodotti, immagini, musica, testi, programmi, giochi, video, film, o di ogni altra opera tutelati a norma di legge.

Il Dirigente Scolastico
Dott. Gianluca Catalano
Firma autografa sostituita a mezzo stampa ai sensi
e per gli effetti dell'art. 3, c. 2, del D.Lgs. 39/93