



Documento di ePolicy

CEIC83800D

I.A.C. "MAZZOCCHI" - S. MARIA C.V.

VIA AVEZZANA EX EGAM - 81055 - SANTA MARIA CAPUA VETERE - CASERTA (CE)

ANTONIO SAPIO

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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 dei ragazzi e delle ragazze 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 online 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 (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di 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.

Argomenti del Documento

1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
 6. Integrazione dell'ePolicy con regolamenti esistenti
 7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
- 2. Formazione e curriculum**
1. Curriculum sulle competenze digitali per gli studenti
 2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
 3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
 4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
- 3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
1. Protezione dei dati personali
 2. Accesso ad Internet
 3. Strumenti di comunicazione online
 4. Strumentazione personale
- 4. Rischi on line: conoscere, prevenire e rilevare**
1. Sensibilizzazione e prevenzione
 2. Cyberbullismo: che cos'è e come prevenirlo
 3. Hate speech: che cos'è e come prevenirlo
 4. Dipendenza da Internet e gioco online
 5. Sexting
 6. Adescamento online
 7. Pedopornografia
- 5. Segnalazione e gestione dei casi**
1. Cosa segnalare
 2. Come segnalare: quali strumenti e a chi
 3. Gli attori sul territorio per intervenire
 4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Informare l'utenza riguardo un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente, è lo scopo del

presente documento di e-policy.

Il fine ultimo della scuola è quello di promuovere l'uso consapevole e critico delle tecnologie digitali e di internet, di far acquisire a tutti gli stakeholders procedure e competenze "tecniche" nonché corrette norme comportamentali e di prevenire, ovvero rilevare e fronteggiare, le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

Gli utenti, soprattutto i minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete; bisogna infatti considerare la possibilità che, durante il lavoro online, si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale.

La Scuola promuove pertanto l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illecite.

Al fine di prevenire il verificarsi di situazioni potenzialmente pericolose, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e, di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa.

1.2 - 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, s'impegni nell'attuazione e promozione di essa.

La nascita di gruppi in rete richiede capacità comunicative e socio-relazionali adeguate. E' quindi fondamentale conoscere come comportarsi in questi gruppi, quali siano le regole da rispettare e quali siano i ruoli e le responsabilità dei soggetti che vi partecipano.

E' auspicabile pertanto che nell'ambito scolastico ci sia chiarezza sui ruoli e sulle responsabilità di ciascun attore del percorso formativo.

Il Dirigente Scolastico garantisce:

- la corretta formazione del personale scolastico tutto sulle tematiche relative all'uso sicuro e consapevole di internet, delle TIC nella didattica e della rete, in linea con il Quadro Normativo di Riferimento e le indicazioni del Miur;
- che si seguano le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione ad incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;
- il suo contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo-cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche;

- l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line e di casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

Il Referente bullismo e cyberbullismo

- coordina le iniziative di prevenzione e di contrasto del "cyberbullismo" (art.4 legge num.71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo");
- promuove iniziative specifiche per la prevenzione ed il contrasto del bullismo e del cyberbullismo avvalendosi della collaborazione delle Forze di Polizia, dell'Università della Campania "Luigi Vanvitelli", della Magistratura, del Tribunale, della Procura e della Diocesi, delle associazioni e dei centri di Aggregazione giovanile presenti sul territorio;
- coinvolge in ambito extrascolastico, con progetti e percorsi formativi, studenti, colleghi e genitori.

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

- promuove la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi (formazione on line);
- monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicura che gli utenti possano accedere alla rete della scuola solo tramite password e riconoscimento su e-proxy;
- cura la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione).

Il personale amministrativo, tecnico ed ausiliario cura:

- il funzionamento dell'istituto scolastico attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola;
- la segnalazione alle famiglie di comportamenti non adeguati e/o episodi di bullismo e cyberbullismo.

I docenti si impegnano a:

- diffondere la cultura dell'uso responsabile delle TIC e della rete;
- promuovere l'uso delle tecnologie digitali nella didattica;
- informarsi ed aggiornarsi sul tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento;
- supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico-educative

(controllo nel rispetto delle leggi, del regolamento interno, del plagio, del diritto d'autore, ecc.);

- garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto dei ruoli e dei codici comportamentali, mediante canali ufficiali e verificabili;

- rispettare l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente;

- interagire con i genitori, coordinando con gli stessi l'intervento educativo collegato all'utilizzo delle tecnologie digitali, nei casi di disagio manifestato dall'alunno;

- segnalare all'Animatore digitale eventuali criticità nei sistemi informativi soprattutto in materia di prevenzione e gestione dei rischi nell'uso delle TIC;

- segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Agli studenti ed alle studentesse è richiesto di:

- utilizzare responsabilmente le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché rispettare le norme codificate nei regolamenti di istituto;

- rispettare le buone pratiche di sicurezza in rete;

- saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui;

- comunicare in rete in modo appropriato rispettando le posizioni altrui;

- partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer-education.

Ai genitori, in continuità con l'istituto scolastico, è richiesto di:

- sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali;

- educare, vigilando sui propri figli, al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo;

- collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

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 studenti e le studentesse. 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 network).

Tutti i soggetti esterni, organizzazioni/associazioni extrascolastiche ed esperti, che a vario titolo, saranno invitati a partecipare alla realizzazione di progetti ed attività educative presso la nostra Istituzione Scolastica dovranno prendere atto di quanto previsto dal documento di E-Policy dell'istituto circa i comportamenti lesivi ed irrispettosi della sicurezza e della privacy del minore e nell'E-policy sottoscrivere un'informativa sintetica del documento in questione.

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

La scuola dovrà assicurare la promozione degli intenti esplicitati nel documento in modo tale che:

- tutti gli alunni siano informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione;
- uno o più moduli di insegnamento sulla e-safety siano programmati nell'ambito delle diverse discipline per l'acquisizione della consapevolezza di un uso sicuro e responsabile di internet;
- l'elenco delle regole per la sicurezza on-line sia pubblicato in tutte le aule o laboratori con accesso a internet;
- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet venga discussa negli organi collegiali (Consigli di classe, Collegio dei Docenti, Consiglio d'Istituto) e comunicata a tutto il personale con il presente documento;
- il personale docente venga reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- un'adeguata formazione dei docenti sull'uso sicuro e responsabile di internet professionalmente e personalmente sia assicurata a tutto il personale;
- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC venga supervisionato dall'Animatore digitale che segnalerà al DSGA eventuali problemi che dovessero richiedere interventi di tecnici.
- l'Animatore digitale metta a disposizione dei docenti le proprie conoscenze;
- tutto il personale sia consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile;
- l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nell'area dedicata presente sul sito web della scuola;
- sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- l'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero;
- i genitori esperti potranno collaborare nelle attività di informazione/formazione del personale e degli alunni.

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

1. Disciplina degli alunni

Gli alunni possono incorrere in determinate infrazioni con l'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica ed in relazione alla fascia di età considerata si elencano le seguenti:

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

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno tanto è vero che, più gli alunni sono piccoli, più i comportamenti "da correggere" sono afferenti ad uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

I provvedimenti "disciplinari" previsti dai docenti proporzionati all'età e alla gravità del comportamento sono:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario e/o registro elettronico;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico;
- prelievo del dispositivo (smartphone o altro device) e consegna all'ufficio di Dirigenza per il ritiro dello stesso da parte dei genitori.

Le figure interessate alla definizione dell'azione da intraprendere sono le seguenti, in ordine di gravità:

- personale scolastico / docente con il coordinatore di classe (bassa entità);
- personale scolastico / docente con il consiglio di classe ed eventuale coinvolgimento della famiglia (media entità);
- personale scolastico / docente con il consiglio di classe, dirigente scolastico e coinvolgimento della famiglia (grave entità);
- personale scolastico / docente con il dirigente scolastico, coinvolgimento della famiglia ed agenti esterni quali le forze dell'ordine e/o la polizia postale (entità gravissima).

La Legge 71/2017, nell'articolo 2, cui si rimanda, indica tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori.

La Legge 71/2017, agli articoli 5 e 7, cui si rimanda, riporta due sanzioni nei confronti dei trasgressori della legge stessa. Per gli studenti minorenni o di età superiore ai quattordici anni sono previste sanzioni disciplinari in ambito scolastico con percorsi di recupero e ammonimento alla famiglia presso le Forze dell'Ordine.

La scuola potrà, altresì, segnalare episodi di cyberbullismo nonché la eventuale presenza di materiale pedopornografico in rete al servizio Helpline di Telefono Azzurro 1.96.96, alla Hotline "Stop-it" di Save the Children, all'indirizzo www.stop-it.it, al fine di trasmettere dette segnalazioni al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.

Le azioni individuate hanno il fine di sostenere le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, e di realizzare interventi educativi nei confronti di coloro che hanno messo in atto comportamenti lesivi del rispetto degli altri.

In ogni caso, i docenti predisporranno specifiche rilevazioni ed azioni preventive sulla base dei protocolli suggeriti dalla piattaforma "Generazioni Connesse", e dei percorsi formativi anche in rete.

A tal fine, sono stati predisposti dei moduli ad hoc reperibili sul loro sito, che costituiscono parte integrante del presente documento.

2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni.

Le potenziali infrazioni sono:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;

- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzo corretto e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

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

Dovere di tutto il personale è collaborare con il Dirigente Scolastico e fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo o penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3) Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli studenti e delle studentesse a scuola, dove si possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Le situazioni familiari meno favorevoli sono:

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

idonei;

- un utilizzo dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni sono soggetti a convocazione a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto ogni anno. Tale monitoraggio viene svolto a cura del Dirigente Scolastico con la collaborazione dell'Animatore Digitale e dei docenti delle classi, tramite questionari e conversazioni.

Il monitoraggio sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti di fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet e sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

L'aggiornamento della policy sarà curato dal Dirigente Scolastico, dall'Animatore Digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La policy richiede l'integrazione con l'inserimento delle seguenti norme:

UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL'UTILIZZO DI INTERNET

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.

3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e la motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. E' vietato cancellare o alterare file-dati presenti sull'hard disk.
8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione...).
9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione all'Animatore Digitale.
10. In caso di malfunzionamento non risolvibile la segreteria contatterà il tecnico informatico esterno.
11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale.
3. E' fatto divieto di usare software non conformi alle leggi sul copyright. E' cura dell'insegnante utente verificarne la conformità. Gli insegnanti possono installare un nuovo software su PC del laboratorio della propria scuola, previa autorizzazione scritta del DS solo se il software installato rispetta le leggi sul copyright.
4. E' responsabilità degli insegnanti, che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.
5. Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

UTILIZZO DEL TELEFONO CELLULARE E DEI VARI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITÀ SCOLASTICHE

- a) Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se malgrado il divieto, gli studenti verranno sorpresi ad usare il cellulare, lo stesso verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e - in collaborazione con il personale ausiliario e/o con la segreteria - convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il cellulare requisito. Avuto inoltre riguardo per il fatto che gli smartphone possono essere utilizzati anche per scattare foto o effettuare riprese filmate, si informano i genitori che eventi di questo tipo, se si concretizzano durante l'orario scolastico, si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.
- b) L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti o agli stessi genitori) né relativamente a smarrimenti e/o sparizioni di telefonini cellulari o di hard/disk portatili o pen drive.
- c) In ogni caso, i genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero in Segreteria.
- d) Il divieto ribadito per i telefoni/videotelefoni cellulari si estende ovviamente anche ad altri oggetti il cui uso a scuola può persino arrecare danni a terzi. A titolo meramente esemplificativo, si citano coltellini di vario genere, attrezzi multiuso con lame richiudibili, sigarette ed accendini ecc.
- e) La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o pen drive o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini / testi / filmati per così dire 'sconvenienti', avendoli scaricati. Per impedire che le stesse postazioni dei laboratori scolastici possano essere furtivamente utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge quindi i visitatori meno esperti. Oltre a questo sofisticato sistema di protezione che blocca l'accesso ai siti di cui si discorre, la scuola ovviamente mette in campo soprattutto la vigile attenzione educativa di ogni singolo docente.

f) Fermo restando il fatto che la scuola è un'istituzione educativa e che non è né prevista né possibile né tantomeno legittima la perquisizione quotidiana di tutti gli studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti. Le responsabilità appena menzionate sono condivise dal personale scolastico dopo aver personalmente constatato o essere venuto a conoscenza che qualche ragazzo/a ha con sé durante l'orario scolastico un oggetto potenzialmente pericoloso e/o il cui uso può compromettere la serenità del clima interno alla scuola.

Ciò al fine di intervenire nelle forme già indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il documento di e-policy sarà aggiornato periodicamente e in tutti i casi in cui si verificheranno cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente e avranno sempre come oggetto di riferimento l'uso consapevole e corretto delle TIC. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si è posto. Il monitoraggio dell'implementazione della Policy e del suo eventuale aggiornamento sarà curato dal gruppo di lavoro con la collaborazione dell'Animatore Digitale e del Referente del bullismo e cyberbullismo, coordinati dal Dirigente Scolastico. Avrà il fine di rilevare le condizioni iniziali delle classi e gli esiti raggiunti a fine anno scolastico, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio on-line sarà rivolto anche ai docenti. Lo stesso avrà lo scopo di valutare l'impatto della Policy e la necessità di eventuali miglioramenti, sul corpo docente. L'aggiornamento dell'e-Policy sarà curato oltre che dal Dirigente Scolastico, dall'Animatore Digitale, dal gruppo di lavoro nonché, dal Responsabile del bullismo e cyberbullismo ed anche dagli Organi Collegiali.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curriculum

2.1. Curricolo sulle competenze digitali per gli studenti

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 alla 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 studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Nel 2006 il Parlamento Europeo ha focalizzato l'attenzione sul Lifelong learning ossia l'apprendimento permanente per tutto l'arco della vita (2006/962/CE). Affinché il cittadino europeo sia attivo e possa pienamente esercitare il suo diritto di cittadinanza, bisogna recepire il quadro comunitario volto ad un processo di riforma educativa.

Il contesto attuale degli stakeholders necessita infatti di un nuovo modello di alfabetizzazione che non sia riduttivo alle sole competenze informatiche ma che traini le nuove generazioni ai raggiungimenti dei saperi necessari per la cittadinanza.

Varie saranno le dimensioni da abbracciare per pensare alle competenze digitali:

DIMENSIONE TECNOLOGICA

La dimensione tecnologica si propone di raggiungere le skills cioè le capacità operative di base nonché i livelli avanzati di potenzialità in contesti tecnologici in trasformazione.

DIMENSIONE COGNITIVA

La dimensione cognitiva mira alle abilità di accesso, selezione, interpretazione e valutazione delle informazioni oltre al saper trattare testi e dati finalizzati alla sintesi, all'analisi e alla rappresentazione con tabelle e grafici.

DIMENSIONE ETICA

La dimensione etica comprende alcune delle tematiche più attuali riguardanti il tema delle nuove tecnologie dalla tutela della privacy al contrasto del fenomeno del cyberbullismo. Si focalizza l'attenzione sulla capacità di interazione con gli altri in modo corretto e responsabile afferente anche alla dimensione relazionale ed affettiva dell'utilizzo di internet.

Ne deriva un concetto di competenza digitale che fa riferimento alla capacità di comprendere ed attuare il potenziale delle tecnologie in un'ottica di costruzione, di conoscenza e promozione della partecipazione e dell'inclusione. Le tecnologie digitali vanno pertanto utilizzate con spirito critico, creativo e consapevole.

Le competenze digitali intese come competenze chiave vanno pertanto individuate e certificate al termine del percorso scolastico in base a quanto normato dal CM n. 3 prot. N. 1235 del 13 febbraio 2015.

Ne è derivato il seguente profilo:

- L'alunno utilizza con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

Il livello raggiunto è identificato dagli indicatori:

A. Avanzato: L'alunno/a svolge compiti e risolve problemi complessi, mostrando padronanza nell'uso delle conoscenze e delle abilità; propone e sostiene le proprie opinioni e assume in modo responsabile decisioni consapevoli.

B. Intermedio: L'alunno/a svolge compiti e risolve problemi in situazioni nuove, compie scelte consapevoli, mostrando di saper utilizzare le conoscenze e le abilità acquisite.

C. Base: L'alunno/a svolge compiti semplici anche in situazioni nuove, mostrando di possedere conoscenze e abilità fondamentali e di saper applicare basilari regole e procedure apprese.

D. Iniziale: L'alunno/a, se opportunamente guidato/a, svolge compiti semplici in situazioni note.

All'interno dell'offerta formativa è stato stipulato un Protocollo d'intesa "Educazione alla Legalità" con enti esterni.

Il percorso intende superare le barriere disciplinari e settoriali per guidare i giovani verso un "nuovo umanesimo". Le attività programmate rientrano nel protocollo stipulato presso la Presidenza del Tribunale di Santa Maria Capua Vetere e che vede uniti 18 partner sul tema dell'educazione degli studenti". I sottoscrittori sono il Comune di Santa Maria Capua Vetere, l'Arcidiocesi di Capua, il Tribunale di Santa Maria Capua Vetere, la Procura della Repubblica, la Questura di Caserta con il locale commissariato di Polizia di Stato, l'Università degli Studi della Campania Dipartimento di

Giurisprudenza, il Consiglio dell'Ordine degli Avvocati, l'Associazione Nazionale Magistrati sezione di Santa Maria Capua Vetere, le dirigenze scolastiche degli istituti di Santa Maria Capua Vetere, l'Ufficio di Sorveglianza di Santa Maria Capua Vetere, il Centro per la Giustizia minorile della Campania e l'ASL di Caserta.

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 studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il servizio scolastico si qualifica tramite la formazione dei docenti e personale tutto; essa rappresenta la solida base per lo sviluppo culturale di tutta l'istituzione.

Il comma 124 della Legge n. 107/2015 dispone: "Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28 marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione, adottato ogni tre anni con decreto del Ministro dell'istruzione, dell'università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria." Il Piano di formazione del personale docente recepisce le criticità emerse dal RAV, le istanze rilevate dal PDM e le proposte indicate nel Piano digitale triennale.

Saranno pertanto previsti momenti di aggiornamento costante e continuo nonché momenti di autoaggiornamento dedicati in particolare all'uso corretto, efficace ed efficiente delle TIC.

Dall'analisi dei bisogni formativi dei docenti, emerge la necessità di intervenire con le seguenti misure:

- Messa a disposizione, di Manuali, Guide e Tutorial per la didattica con le TIC;
- Condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale e del Team per l'innovazione previsto dal PNSD.

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 online. 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) e 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.

Coerentemente con quanto previsto dal PNSD, ed in modo particolare con l'azione #28, la nostra Scuola si avvale dell'Animatore Digitale, una figura di sistema, che con il Dirigente Scolastico e il Direttore S.G.A. opererà per concretizzare gli obiettivi e le innovazioni del PNSD nella vita scolastica. Nasce quindi la necessità di una formazione specifica affinché possa (rif. Prot. n.17791 del 19/11/2015) "favorire il processo di digitalizzazione delle scuole nonché diffondere le politiche legate all'innovazione didattica attraverso azioni di accompagnamento e di sostegno sul territorio del piano nazionale scuola digitale". Per quanto riguarda la formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, l'Istituto ha individuato docenti opportunamente formati in merito ai temi:

- Le mafie
- Bullismo e cyberbullismo
- Lotta alle dipendenze
- Ambiente

L'istituto ha previsto momenti di autoformazione e di formazione collettivi di carattere permanente.

Per realizzare gli interventi previsti dal PNSD la scuola agirà su più fronti:

- organizzare corsi interni, sia predisposti dall'Istituto che da scuole in rete;
- favorire la partecipazione a corsi esterni inerenti la didattica innovativa per ogni singola disciplina e/o che rispondano ad esigenze formative del sistema scolastico nel suo complesso;
- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi.

Si farà ricorso, volta per volta e secondo le esigenze, alle risorse sotto indicate:

- personale docente interno alla scuola che abbia acquisito competenze in determinati settori affini alle esigenze sopra evidenziate;

- soggetti esterni che offrano la possibilità di mettere in opera un'attività di consulenza mediante seminari e incontri-dibattito;

- formazione a distanza.

Sarà consentita la partecipazione ad iniziative al di fuori della pianificazione d'Istituto, in coerenza con le finalità e gli obiettivi del Piano.

2.4. - Sensibilizzazione delle famiglie e integrazioni al 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 ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Sul sito web dell'istituto, a disposizione delle famiglie sono ben individuate le attività svolte dalla scuola finalizzate al successo scolastico ed educativo di ogni studente.

Il Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni, sancisce infatti l'impegno reciproco di scuola e famiglia alla corresponsabilità formativa.

Presenti inoltre i temi legati alla eSafety.

Verranno valorizzate le opportunità di incontro e formazione delle famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative da enti e/o associazioni di comprovata affidabilità.

Il coinvolgimento dell'intera comunità scolastica è parte integrante del PTOF ed è una delle misure individuate nel piano d'azione proposto da "Generazioni Connesse".

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con particolare riferimento alla prevenzione del cyberbullismo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)

- Organizzare incontri con esperti per i docenti sulle competenze digitali

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati

personali.

La scuola deve sempre rispondere ai principi della sicurezza sia per quanto riguarda l'ambiente fisico che l'ambiente online.

Bisogna sempre considerare prioritaria la questione della rete wireless e non, degli account degli utenti (siano essi studenti, insegnanti o personale ATA), l'hardware, il software e la privacy. In riferimento all'hardware, la scuola si avvale di un tecnico esterno che periodicamente effettua manutenzione di aggiornamento e ripristino. Nella scuola ogni plesso è dotato di aule attrezzate di LIM.

Per quanto riguarda la protezione dei dati personali si fa riferimento al "Codice della Privacy" DL n. 196 del 30 giugno 2003, e dal GDPR (General Data Protection Regulation) n. 679 del 2016.

All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola (Allegato 1). A tale proposito si evidenzia che le immagini e le riprese audiovideo realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati. Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre dello stesso anno, la scuola non si impegna solo a tutelare la privacy degli/le studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di sé stessi e degli altri.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*

4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'accesso a Internet è libero solo per gli ambienti di segreteria e di presidenza che, peraltro, risultano protetti da software antivirus. L'accesso attraverso WI-FI è protetto da password e da un proxy. Sui dispositivi tablet e sui computer sono stati limitati gli accessi a siti sicuri.

Gestione accessi (password, backup, ecc.)

L'accesso ai portali istituzionali come SIDI, Istanze on-line, alla Segreteria Digitale, PON ecc. prevede l'uso di credenziali personali, mentre l'accesso a portali tematici si effettua per mezzo di password uniche condivise tra i referenti di progetti e/o azioni e la dirigenza. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. Anche ai genitori sono state fornite credenziali personali di accesso al registro elettronico. Il backup viene eseguito dal sistema periodicamente e i dati preservati in cloud. I dati personali vengono trattati nel rispetto della normativa sulla privacy.

Posta elettronica

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo. I docenti utilizzano per scopi didattici il proprio account su dominio posta.istruzione.it o mazzocchiscuola.edu.it (GSuite). La posta elettronica è protetta da antivirus e

da antispam.

Sito web della scuola

La scuola è dotata di un sito istituzionale con estensione "gov.it" che verrà sostituito a breve con quello "edu.it" (già funzionante ma in manutenzione) sul quale diversi siti tematici rimandano al contenuto di interesse. Per mezzo di credenziali personali si accede all'area riservata per la presa visione di circolari e comunicazioni ufficiali. Pulsanti attivi permettono l'accesso a link di interesse tra cui il Registro Elettronico inoltre è possibile trovare "Regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari".

Socialnetwork

Attualmente nella didattica in presenza non si utilizzano social network, neanche da parte dell'istituzione scolastica, e il personale scolastico non è autorizzato a utilizzarli per nome e per conto della stessa.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Al fine di facilitare e favorire un approccio collaborativo a scuola si fa ricorso alle tecnologie digitali.

E' propria della nostra epoca la necessità di una comunicazione digitale maggiormente interattiva ed orizzontale.

Il primo contatto avviene tramite il sito dell'I. C. A. S. Mazzocchi raggiungibile all'indirizzo www.mazzocchiscuola.gov.it, che a breve sarà sostituito con www.mazzocchiscuola.edu.it (in manutenzione). A cura del DS e dei docenti referenti del sito web ci sono la gestione del sito e la rispondenza alle normative vigenti in base ai contenuti dell'accuratezza, dell'appropriatezza e dell'aggiornamento. Sul sito sono pubblicati il regolamento d'Istituto, il RE, gli avvisi ai genitori, gli eventi. Tramite l'accesso all'area riservata, si viene a conoscenza delle comunicazioni interne e della modulistica.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Per gli studenti: gestione degli strumenti personali

Come evidenziato nel "Patto di Corresponsabilità", si fa divieto a chiunque di utilizzare il telefono cellulare durante le ore di lezione. Qualora gli studenti avessero necessità di comunicare con i familiari, previa autorizzazione del docente presente in classe, si recheranno in segreteria dove potranno usufruire del centralino della scuola. Il divieto è inteso anche per fare foto o video non autorizzati", coerentemente con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007.

Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni della presente policy.

Per i docenti: gestione degli strumenti personali

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo tra quelli scolastici disponibili.

Per il personale ATA: gestione degli strumenti personali

E' vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei

docenti.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

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

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

Si individuano i principali rischi legati ad un utilizzo non consapevole del digitale e delle Rete nei quali può incorrere il minore.

Tutta la comunità educante viene posta di fronte alla sfida di individuare la propria identità, le proprie risorse ed il proprio ruolo educativo. L'Istituto Comprensivo Mazzocchi per formare le competenze educative di base per la corretta gestione delle situazioni di vita dei ragazzi online, intende perseguire azioni di prevenzione universale e di sensibilizzazione, attraverso la rete dei servizi territoriali locali.

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 studenti (ed ex studenti) 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;
- Il sistema scolastico deve prevedere 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).

Il bullismo riguarda tutte quelle situazioni di aggressione volontaria e ripetuta finalizzata ad insultare, minacciare, diffamare o ferire una persona o un piccolo gruppo. Se questi comportamenti si reiterano on line si sfocia nel cyberbullismo che può essere:

- Invasivo (il bullo raggiunge la vittima sempre e ovunque)
- Persistente (tutto ciò che viene messo in rete, difficilmente può essere cancellato)
- Esteso (la platea che assiste è potenzialmente illimitata).

Il Comprensivo Mazzocchi si prefigge di adottare, a seconda dei casi, azioni di prevenzione:

- Universale (partendo dal presupposto che tutti gli studenti sono potenzialmente a rischio)
 - Selettiva (se sono stati individuati casi attraverso indagini o segnalazione fatta alla scuola)
 - Indicata (per la riduzione di comportamenti problematici e per dare supporto alla vittima).
-

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 online) 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, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti 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.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

L'Hate speech o "incitamento all'odio" o ancora "discorso d'odio", indica discorsi tra cui post, immagini, commenti etc. e pratiche non solo online che esprimono odio e intolleranza verso un gruppo o una persona che possono essere identificate come appartenente a un gruppo o categoria e che rischiano di provocare reazioni violente concatenate tra loro.

Per estensione il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione di tipo razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità eccetera ai danni di una persona o di un gruppo. E' necessario affrontare tale fenomeno sempre più diffuso anche a livello educativo e scolastico al fine di:

- fornire agli studenti 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 posizione consapevole e costruttiva da parte dei giovani.

Vengono di seguito descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica:

1. Potenziare lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie per la promozione della consapevolezza di queste dinamiche in rete.
2. 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;
3. promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
4. favorire una presa di posizione consapevole e costruttiva da parte dei giovani.

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...).

4.4 - Dipendenza da Internet e gioco online

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 attraverso percorsi sul benessere digitale?

La Dipendenza da Internet relativa all'utilizzo eccessivo e incontrollato di Internet, al pari di altri comportamenti patologici o dipendenze, può causare o essere associato ad isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

Tale dipendenza, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica, che deve focalizzare l'attenzione sul fenomeno e fornire gli strumenti agli studenti e alle studentesse 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 online,
- 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.

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. Sarà inoltre fondamentale concordare una linea unica 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 medialità sessualmente espliciti; i/le ragazzi/e 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.

I contenuti sessualmente espliciti, condivisi tramite immagini o video in modo talvolta incontrollabile e inconsapevole, possono diventare materiale di ricatto assumendo la forma di "revenge porn" che tra i rischi contempla:

- violenze psicosessuali
 - umiliazioni
 - bullismo
 - cyberbullismo
 - molestie
 - stress emotivo
 - ansia e depressione.
-

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente 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 online, 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 online.

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 seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

L'adescamento on line vede coinvolti ragazzi e ragazze che spesso manifestano scarsa educazione emotiva, sessuale e assenza di competenza digitale. Bisogna, pertanto, al fine di prevenire tale fenomeno, accompagnarli in un percorso di educazione all'affettività e alla sessualità (anche digitale). Gli adulti di riferimento (genitori, docenti ecc.), quando hanno la certezza dell'adescamento on line, non si devono assolutamente sostituire al minore perché potrebbero compromettere eventuali prove e dovrebbero rivolgersi alla Polizia Postale e delle Comunicazioni. Importante in questo caso anche l'intervento di un Servizio territoriale (Consultorio familiare, Servizio di Neuropsichiatria infantile...) per supportare psicologicamente la vittima. Quest'ultima non si deve sentire giudicata ma compresa e ascoltata per cercare di arginare il senso di colpa.

4.7 - Pedopornografia

La pedopornografia online 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](#).

Qualora ci fosse accertato caso di pedopornografia le autorità competenti, appena ricevuta la segnalazione, hanno l'obbligo di rimuovere il materiale dalla Rete e di adoperarsi affinché vengano individuati i responsabili e identificati altri minori abusati presenti nelle immagini o nei video.

Le figure di riferimento potranno dare indicazioni in merito ad un primo supporto psicologico per salvaguardare il benessere psicofisico delle vittime per poi appoggiarsi ai servizi socio-sanitari del territorio di appartenenza. Le Forze dell'Ordine diverranno così supporto indispensabile e immediato quando vengono a conoscenza di tale tipologia di reato. Il materiale pedopornografico anticipa l'abuso sessuale ed è quindi fondamentale prevenire quest'ultimo. L'abuso sessuale on line si fonda sul ruolo delle tecnologie digitali che diventano il mezzo attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con effetti sulle vittime che si aggiungono e si moltiplicano a quelli associati all'abuso sessuale.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, 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.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

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

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

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

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 online.

Qualora il minore dovesse riferire al docente eventi o fatti accaduti anche al di fuori della scuola, bisognerebbe prendere in considerazione i punti da segnalare:

- 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, ecc.);

- 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, ecc.);

- 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), ecc.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse 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.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Il nostro Istituto ha individuato una figura referente per il cyberbullismo alla quale arriverà la segnalazione da parte del singolo docente mediante il modulo scaricabile dal link nella sezione "Altri Allegati" del presente documento.

Il referente ed il team per le emergenze dopo aver raccolto le informazioni utili, anche attraverso colloqui con gli attori coinvolti, interesserà il Dirigente che valuterà se la segnalazione debba essere rivolta agli organi esterni quali la Polizia Postale, i servizi sociali o se il caso può essere gestito dal Consiglio di Classe con la partecipazione delle famiglie degli alunni coinvolti. Si sceglieranno poi, gli interventi da attuare a cui seguirà una fase di monitoraggio (Allegato 2)

5.3. - *Gli attori sul territorio*

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

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" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

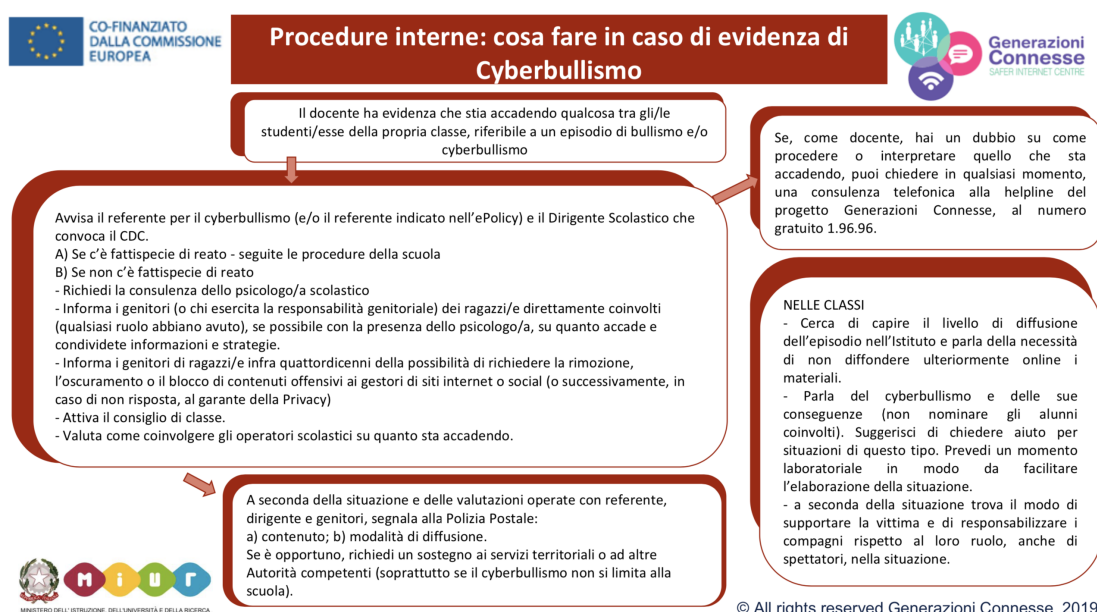
alla tutela dei minori.

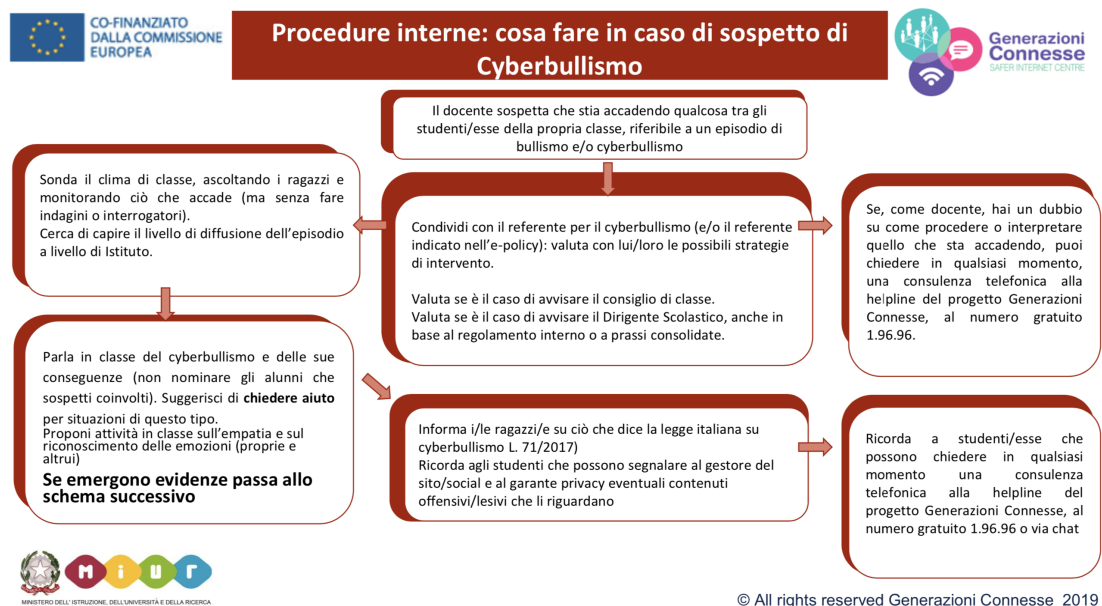
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete 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. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **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.

I documenti relativi alle procedure operative e i protocolli sono da elaborare in collaborazione con i suddetti attori del territorio, con cui siglarli unitamente.

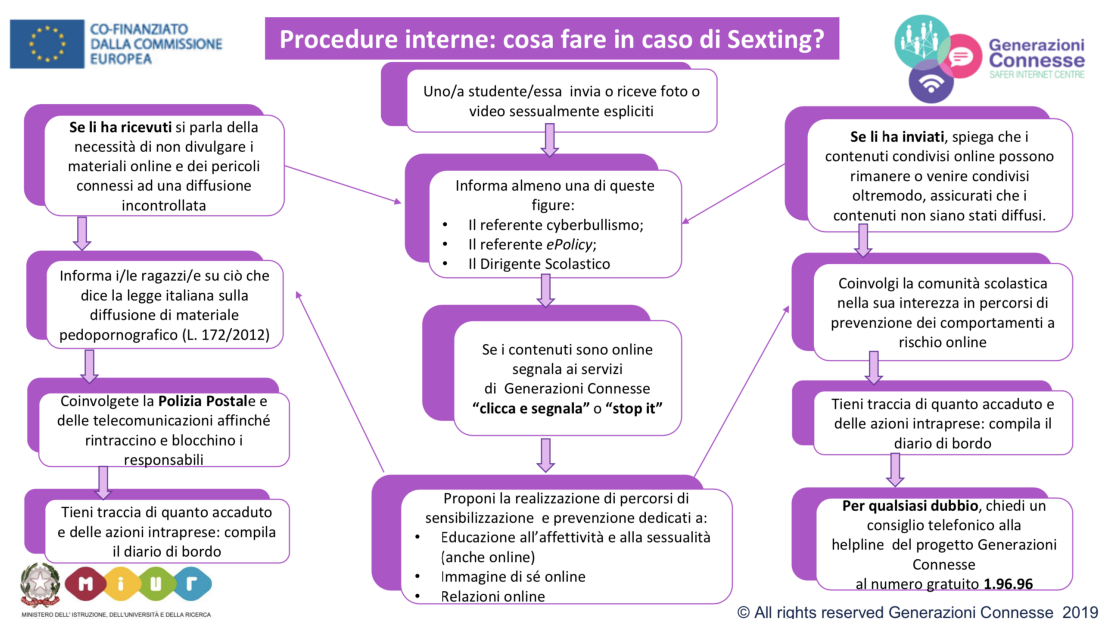
5.4. - Allegati con le procedure

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?

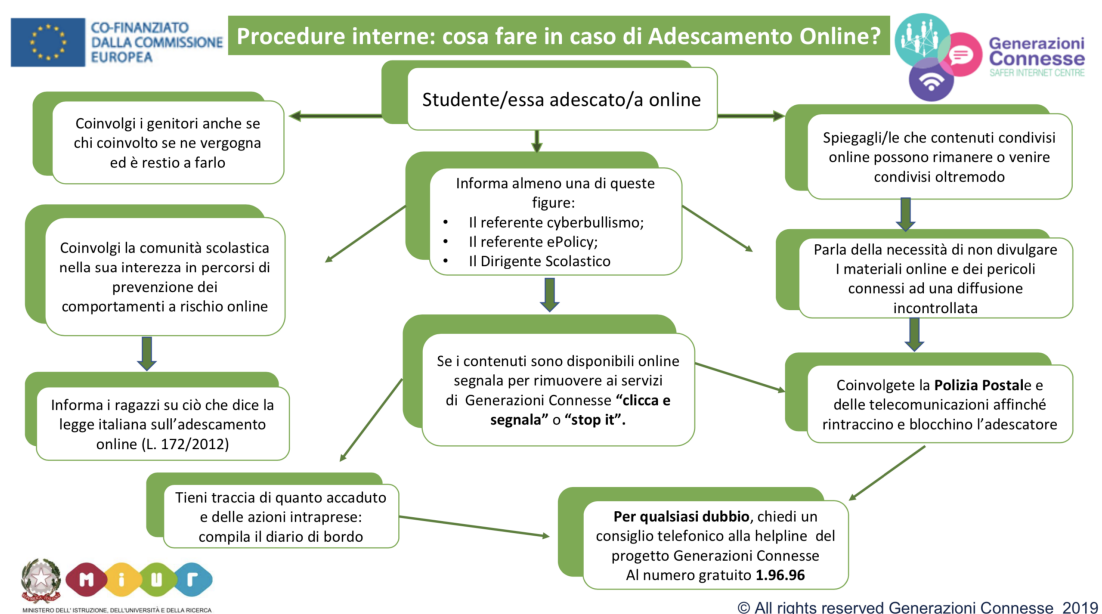




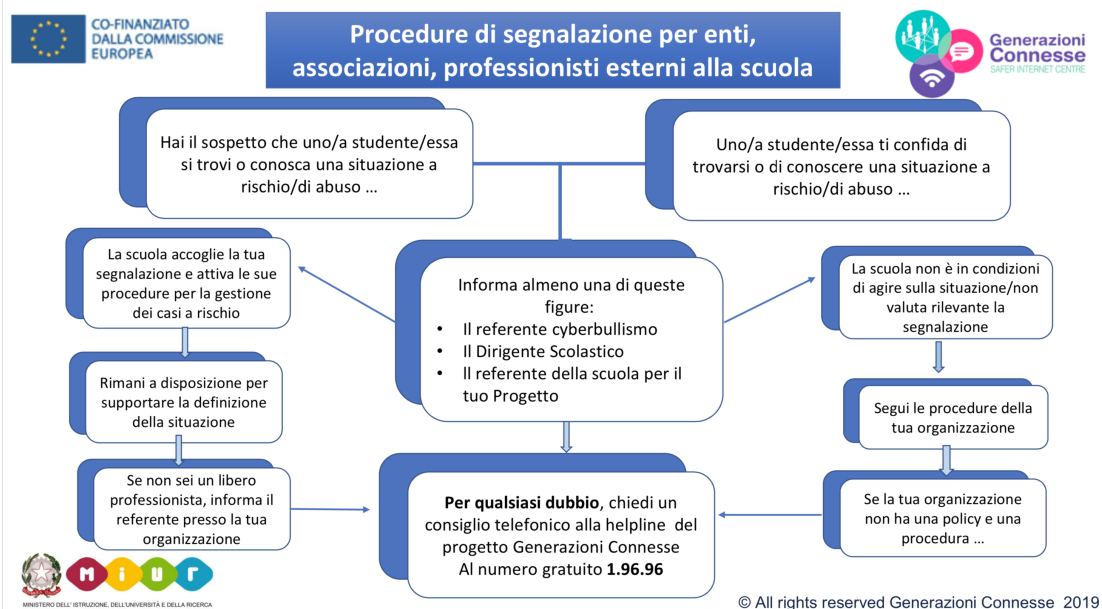
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- [Scheda di segnalazione](#)

- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

ALLEGATO 1 Modulo liberatoria immagini e video degli alunni - Tutela della privacy

**PLESSO EX EGAM - scuola secondaria di I grado e uffici amministrativi: Via
Avezana - 0823845912 fax 0823795914**

**PLESSO S. ERASMO - scuola dell'infanzia, primaria e secondaria di I
grado: Via Mascagni tel-fax 0823799505**

**PLESSO S.ANDREA - scuola dell'infanzia e primaria: P.zza Giovanni
XXIII tel 0823898090**

**E-MAIL: ceic83800d@istruzione.it SITO WEB
<http://www.mazzocchiscuola.gov.it>**

**C.F. 80005970613
DISTRETTO 16**

**TUTELA DELLA PRIVACY DEI MINORI
DICHIARAZIONE LIBERATORIA PER FOTOGRAFIE E RIPRESE
VIDEO**

Resa dai genitori degli alunni minorenni

**Regolamento (UE) N° 679/2016 sulla protezione dei dati
personali**

Io sottoscritto _____, nato a
_____ (_____),
il _____ / _____ / _____, residente a
_____ (_____),
indirizzo: _____

_____;
Io sottoscritto _____, nato a
_____ (_____),
il _____ / _____ / _____, residente a
_____ (_____),
indirizzo: _____

_____;
genitori/esercenti la patria potestà dell'alunno _____
frequentante la classe _____ sez. _____

AUTORIZZIAMO

☒ ☒ L'istituto Comprensivo Statale "A.S. Mazzocchi" nella persona del
Dirigente Scolastico, titolare del trattamento ai sensi dell'art. 13 del GDPR,
all'effettuazione e all'utilizzo di fotografie, video o altri materiali audiovisivi
contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di

attività educative e didattiche dell'Istituto Scolastico per scopi documentativi, formativi e informativi. Il Dirigente Scolastico dell'Istituto Comprensivo Statale "A.S. Mazzocchi" assicura che le immagini e le riprese audio-video realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite pubblicazioni, mostre, corsi di formazione, concorsi, seminari, convegni e altre iniziative promosse dall'Istituto anche in collaborazione con altri enti pubblici, o associazioni. Voi potrete in ogni momento esercitare i diritti di cui agli artt.15,16,18,20,21 del Regolamento UE. Nel caso di partecipazione dell'Istituto ad eventi pubblici, come concerti, premiazioni ed altre manifestazioni a cui accedano soggetti esterni che svolgono attività giornalistica, si solleva L'istituto Comprensivo "A.S. Mazzocchi" da ogni responsabilità sul trattamento, in quanto non titolare, di eventuali dati di cronaca, immagini e riprese. La presente autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la dignità personale ed il decoro del minore e comunque per uso e/o fini diversi da quelli sopra indicati. Il/la sottoscritto/a conferma di non aver nulla a pretendere in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

Luogo e data _____
fede

In

(firma di entrambi i genitori)

Allegati:

- fotocopie dei documenti d'identità

Allegato 2

PROCEDURA PER CASO DI PRESUNTO BULLISMO E VITTIMIZZAZIONE A SCUOLA:

1. Segnalazione dell'episodio da parte del docente o referente bullismo/coordinatore E-policy
2. Valutazione del caso
3. Gestione del caso attraverso uno o più interventi:
 - Approccio educativo con la classe
 - Intervento individuale con gli attori coinvolti
 - Coinvolgimento della famiglia
 - Coinvolgimento di esperti esterni (psicologi, enti specializzati, polizia postale)

4. Monitoraggio

ALLEGATO 3

Procedure operative per la gestione delle infrazioni e relative sanzioni.

Qualora un membro del personale o studente violi la E-Safety Policy, il Dirigente Scolastico stabilirà il livello di sanzioni da applicare individuando le corrette procedure comportamentali e disciplinari della scuola.

Di seguito sono fornite alcune procedure operative come esemplificazione:

STUDENTI:

INFRAZIONI

- L'uso non autorizzato del telefono cellulare (o di altre nuove tecnologie) durante le lezioni.
- Uso di instant messaging / Siti di social networking.
- L'uso non autorizzato di e-mail dopo essere stato avvertito.
- L'uso non autorizzato del telefono cellulare (o di altre nuove tecnologie) durante le lezioni.
- Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.
- Trasmissione di materiale che violi i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.

PROVVEDIMENTI IMMEDIATI

- Rimozione del telefono fino a fine giornata;
- Segnalazione al Dirigente Scolastico;
- Contatto con i genitori;
- Contatto con le autorità competenti per i casi più gravi.

SANZIONI

Le sanzioni saranno erogate nel rispetto del "Regolamento d'Istituto" presente sul sito della scuola.

AZIONI DI SALVAGUARDIA

1. Conservare le prove;
2. Informare i provider di servizi di posta elettronica tramite l'animatore digitale;
3. Fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati, dovrà informare il Dirigente Scolastico, il referente del cyberbullismo o il coordinatore

dell'E-safety anche attraverso la compilazione di una "scheda di segnalazione". La scheda di segnalazione potrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno o comunicati da terzi.

PERSONALE SCOLASTICO:

INFRAZIONI:

- L'uso di Internet per attività personali non legate allo sviluppo professionale (shopping online, email personali, instant messaging ecc).
- L'utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato.
- Qualsiasi comportamento su Internet che compromette la professionalità del personale nella scuola e nella comunità.
- L'uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password.
- Violazione del copyright o della licenza per l'installazione di software.
- Gravi danni intenzionali all'hardware o software del computer.
- Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica.
- Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.
- Ricevere o trasmettere materiale che violi i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.
- Portare il nome della scuola in discredito

PROVVEDIMENTI IMMEDIATI

- Avvertimento verbale da parte del Dirigente Scolastico;
- Rapporto alle autorità competenti.

Fare segnalazione al Coordinatore dell'E-Safety/ DSGA / Dirigente Scolastico.

Altre azioni di salvaguardia:

1. rimuovere il PC in un luogo sicuro per garantire che non vi sia alcun ulteriore accesso al PC o laptop;
2. far verificare tutte le attrezzature per garantire che non vi sia alcun rischio di alunni che accedano a materiali inappropriati nella scuola.

Il nostro piano d'azioni

Non è prevista nessuna azione.

