Documento di ePolicy

ICS Mons.P.Guerriero – Avella

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** figurano fra le abilità chiave annoverate 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). Esse inoltre vengono direttamente richiamate dalla recente normativa che ha introdotto l'insegnamento dell'Educazione Civica in tutte le scuole di ogni ordine e grado allorquando si parla di *Cittadinanza digitale* (LEGGE 20 agosto 2019, n. 92 *Introduzione dell'insegnamento scolastico dell'educazione civica*).

Inoltre, quando parliamo di uso corretto della Rete non si può prescindere dalla più recente normativa sulla *Didattica Digitale Integrata*, parte del più ampio *Piano Scuola 2020/2021* (D.M. n. 39 del 26 giugno 2020), nato da esigenze gestionali scaturite dalla pandemia da Covid-19. Tale contingenza ha proiettato la scuola italiana in un contesto di apprendimento legato alle nuove tecnologie del tutto nuovo e, fino alla primavera 2019, del tutto marginale rispetto al quotidiano fare d'aula.

In un contesto sempre più complesso, è diventato quindi essenziale per ogni Istituto Scolastico dotarsi di una ePolicy, un documento programmatico volto da un lato a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole da parte dei ragazzi e delle ragazze della nostra Istituzione scolastica, e dall'altro, per gli adulti coinvolti nel processo educativo – in primis docenti e genitori - a prevenire situazioni problematiche e a riconoscere, monitorare, segnalare e gestire episodi legati ad un utilizzo scorretto degli strumenti elettronici.

L'ePolicy ha l'obiettivo di esprimere la visione educativa e la proposta formativa del nostro Istituto, 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.

Indice degli argomenti:

Presentazione dell'ePolicy

Scopo dell'ePolicy

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

Lo scopo di questo documento è, inoltre, quello di esporre le linee guida per la prevenzione e il contrasto di fenomeni devianti quali quelli del ***bullismo*** e ***cyberbullismo*** all'interno del nostro Istituto, in conformità con le *Linee di orientamento* emanate dal MIUR nell'ottobre del 2017; esso intende fornire ai docenti uno strumento di lavoro che risponda alle sfide educative e pedagogiche indotte dall'evolversi costante dell'uso delle nuove tecnologie, ed ai genitori un punto di riferimento chiaro e puntuale nell'affrontare scenari problematici riconducibili ad atti di bullismo e/o cyberbullismo in cui possono rimanere coinvolti i loro figli, sia come possibili soggetti attivi che come possibili soggetti passivi. E'pertanto necessario avviare una politica di sicurezza della navigazione *on line* volta ad un controllo dell'uso delle strumentazioni digitali e alla diffusione di buone pratiche di comunicazione sui *social network* da parte dei nostri alunni.

Il presente documento è stato realizzato tenendo conto delle indicazioni fornite dal progetto *Generazioni connesse* (www.generazioniconnesse.it) realizzato su indicazioni del MIUR e della Commissione europea col supporto della Polizia Postale, del Garante per l'Infanzia e delle associazioni che operano in difesa dei diritti dei ragazzi.

Riferimenti normativi

Il ***bullismo*** e il ***cyberbullismo*** devono essere conosciuti e combattuti così come previsto:

- dall' art. 3 della Costituzione italiana (Principio di uguaglianza);
- dall'art. 34 della Costituzione italiana (Diritto allo studio);
- dalla Direttiva Ministeriale n.16 del 5 febbraio 2007 recante *Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo*;
- dalla direttiva Ministeriale n. 30 del 15 marzo 2007 recante *Linee di indirizzo ed indicazioni in materia di utilizzo di 'telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti*;
- dalla direttiva Ministeriale n. 104 del 30 novembre 2007 recante *Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali*;
- dal D.P.R. 249/98 e 235/2007 recante *Statuto delle studentesse e degli studenti*;
- dalle *Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo,* MIUR aprile 2015;
- (tra gli altri) dagli art. 581 (percosse) - 582 (lesione personale) - 595 (diffamazione) - 610 (violenza privata) - 612 (minaccia)- 635 (danneggiamento) del Codice Penale;
- dagli art. 2043 (risarcimento per fatto illecito) - 2047 (danno cagionato dall'incapace) – 2048 (responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte) del Codice Civile.
- dalla Legge 107 del 2015;
- dalla Legge del 29 maggio 2017 n.71 - *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*;

- dalle *Linee di orientamento per la prevenzione e il contrasto del cyberbullismo*, MIUR ottobre 2017;
- dalle *Linee di orientamento per la prevenzione e il contrasto del cyberbullismo*, MIUR (Decreto ministeriale 18 del 13 gennaio 2021 emanato con nota 482 del 18 febbraio 2021).

Ruoli e responsabilità

Ruoli	**Responsabilità**
Dirigente Scolastico: responsabile per la sicurezza dei dati e garante dell'applicazione della ePolicy	✔ individua attraverso il Collegio dei Docenti un *Referente del bullismo e cyberbullismo*; ✔ coinvolge nella prevenzione e contrasto al fenomeno del bullismo/cyberbullismo, tutte le componenti della comunità scolastica. ✔ favorisce la discussione all'interno della scuola, attraverso gli organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e la prevenzione dei fenomeni del bullismo e del cyberbullismo.
Referente Bullismo e Cyberbullismo:	✔ promuove attività, eventi funzionali alla prevenzione delle problematiche inerenti al cyberbullismo.
Animatore Digitale, supportato dal Team per l'innovazione digitale:	✔ stimola 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; ✔ monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola, nonché propone la revisione delle politiche dell'Istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola; ✔ assicura che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate; ✔ coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla *scuola digitale*.
Docenti:	✔ si informano/aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; ✔ fanno in modo che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi; ✔ garantiscono che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di

	comportamento professionale ed effettuate con sistemi scolastici ufficiali; ✔ controllano l'uso delle tecnologie digitali da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); ✔ nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni su siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei; ✔ comunicano ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo; ✔ segnalano al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme;
<u>Personale ATA:</u>	✔ garantisce il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet.
<u>Genitori:</u>	✔ sostengono la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica; ✔ seguono gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti e, più in generale, dalla scuola; ✔ concordano con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet; ✔ fissano delle regole per l'utilizzo del computer e tengono sotto controllo l'uso che i figli fanno di Internet e del cellulare in generale.
<u>Alunni:</u>	✔ sono responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti; ✔ comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi; ✔ adottano condotte rispettose degli altri anche quando si comunica in rete;

	✔ esprimono domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet, ai docenti e ai genitori.

Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il presente documento di ePolicy è pubblicato sulla HomePage del sito della scuola (www.icavella.it) dopo essere stato approvato dal Collegio dei Docenti e dal Consiglio d'Istituto.

Gestione delle infrazioni alla ePolicy

Nel caso in cui una violazione al *Regolamento di Istituto* si configuri come atto di *bullismo* e\o *cyberbullismo,* colui che ne viene a conoscenza informa tempestivamente il Dirigente Scolastico e il Referente per il bullismo e il cyberbullismo. Qualora tali infrazioni dovessero configurarsi come reato, il Dirigente Scolastico farà una tempestiva segnalazione all'Autorità Giudiziaria in quanto gli è attribuita qualità di Pubblico Ufficiale ai sensi dell'art.357 del Codice di Procedura Penale. (vedi sez. *Segnalazione e gestione dei casi – protocollo attuativo* p. 14)

Si rinvia al *Regolamento d'Istituto,* al *Patto di Corresponsabilità* e allo *Statuto delle Studentesse e degli studenti*.

Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

Il monitoraggio dell'implementazione della ePolicy e il suo eventuale aggiornamento saranno svolti ogni anno.

Il monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Referente per il bullismo e cyberbullismo e dai docenti delle classi, anche tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della ePolicy e la necessità di eventuali miglioramenti.

L'aggiornamento della ePolicy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dal Referente per il bullismo e cyberbullismo e dagli Organi Collegiali, a seconda degli aspetti considerati.

Integrazione dell'ePolicy con regolamenti esistenti

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

- Disposizioni sull'uso del ***laboratorio di informatica fisso o portatile, delle postazioni di lavoro e dell'utilizzo di Internet.***

- Decreto Ministeriale n.89 del 07 agosto 2020 recante *Adozione delle linee guida sulla Didattica digitale integrata, di cui al Decreto del Ministero dell'Istruzione26 giugno 2020, n.39.*

Formazione e curricolo

Curricolo sulle competenze digitali per gli studenti

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.

Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la *competenza digitale* è ritenuta dall'Unione Europea *competenza chiave*, per la sua importanza e pervasività nel mondo d'oggi.

Il Decreto legge del 22/06/2020 ha inoltre stabilito che dall'anno scolastico 2020/2021 entri in vigore il nuovo insegnamento di Educazione Civica – 33h previste all'interno del curricolo scolastico di ogni ordine e grado – al cui interno è previsto l'insegnamento volto alla *cittadinanza digitale*, affinchè alle nostre alunne e ai nostri alunni vengano forniti gli strumenti per utilizzare consapevolmente e responsabilmente i nuovi mezzi di comunicazione e gli strumenti digitali, in un'ottica di sviluppo del pensiero critico e di sensibilizzazione rispetto ai possibili rischi connessi all'uso dei social media e alla navigazione in Rete, nonché di contrasto del linguaggio dell'odio.

Competenza digitale significa dunque padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con *autonomia e responsabilità* nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

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

Il nostro corpo docente ha preso parte a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze; nel caso delle figure di sistema, esse si configurano come di carattere specialistico. E' inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali appositamente create, e corsi di aggiornamento online.

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

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, prevede momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi. Sarà predisposta una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento

sull'utilizzo consapevole e sicuro di Internet, collegata alla homepage del sito scolastico, fruibile attraverso l'inserimento di una password cliccando sul link in homepage. Qui è possibile trovare materiali informativi sulla sicurezza in Internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse", ecc.

Sensibilizzazione delle famiglie e Patto di corresponsabilità

L' Istituto attiva iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza del *Patto di corresponsabilità* dell'ICS – nella parte riguardante sia i diritti che i doveri legati alle varie figure facenti parte del processo educativo - e delle numerose situazioni di rischio online. A tal fine i docenti mettono a disposizione dei genitori materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a *Generazioni connesse* saranno messi in condivisione materiali dedicati ad alunni e famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il Regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto di Internet.

Gestione dell'infrastruttura e della strumentazione ICT della scuola.

Protezione dei dati personali

Sono *dati personali* le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti *sensibili*, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti *giudiziari*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

I *soggetti* sono:

- L'interessato, che è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);
- Il titolare, che è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);
- Il responsabile, che è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Trattamento dei dati è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insieme di dati personali come, ad esempio, la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento UE 2016/679).

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantirne il corretto e sicuro utilizzo.

Il nostro Istituto Scolastico in conformità al *Regolamento UE 2016/679* deve:

- redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti;
- valutare i rischi sulla privacy: (definita nel regolamento *Data Protection Impact Assessment* o *PIA*) relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e, come i dati vaccinali con le Asl;
- analizzare il processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti;
- adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti;
- analizzare il sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati;
- mettere in sicurezza la rete intranet scolastica;
- utilizzare *black list* per la navigazione (sistemi di filtraggio dei contenuti);
- utilizzare un *firewall hardware* (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole);
- istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub-incaricati del trattamento.

Accesso a internet

L'accesso a Internet è possibile e consentito per la didattica nei laboratori multimediali fissi e/o portatili. Solo il docente dalla propria postazione può consentire agli alunni di accedere a Internet. Le postazioni sono settate in maniera tale che il consenso da parte degli utenti all'utilizzo di webcam e microfono non avvenga automaticamente ma sia subordinato all'autorizzazione del docente responsabile. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a *black list* o consentono il collegamento solo a siti idonei alla didattica, secondo le impostazioni date dall'Animatore digitale che periodicamente provvede alla manutenzione e aggiornamento del sistema informatico del laboratorio, ove necessario richiedendo l'intervento di tecnici esterni. Le postazioni degli alunni (client) sono occasionalmente utilizzate anche dai docenti, quando questi si servono dei laboratori. I docenti hanno piena autonomia nel collegamento ai siti web.

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.

Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali e non che a vario titolo sono inserite 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.

- **Per gli studenti**: gestione degli strumenti personali – cellulari, tablet ecc.

  Per gli studenti della Scuola primaria: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche.
  Per gli studenti della Scuola secondaria di primo grado: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche (intervalli inclusi). E' consentito agli alunni con *Bisogni Educativi Speciali* utilizzare il proprio notebook o tablet, senza connessione Internet, previa richiesta scritta del genitore, concordando con i docenti le modalità. È consentito a tutti gli alunni, in casi specifici concordati con il docente (uscite didattiche, produzioni multimediali...) l'utilizzo di dispositivi elettronici personali per scopi didattici.

- **Per i docenti**: gestione degli strumenti personali– cellulari, tablet ecc.

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

- **Per il personale della scuola**: gestione degli strumenti personali– cellulari, tablet ecc.

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

Rischi on line: conoscere, prevenire e rilevare

Sensibilizzazione e prevenzione

Per i ragazzi *nativi digitali* le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi *media*. Le tecnologie digitali offrono da tempo la possibilità di ampliare la propria rete di amicizie in modo quasi smisurato: non è infrequente che gli adolescenti "si sfidino" tra loro rispetto al numero di *amicizie* strette online. Avere molti amici nella *vita virtuale*, o molti *followers*, è elemento di grande popolarità e di vanto con gli amici della *vita reale*. Non a caso, quindi, gli adolescenti aggiungono tra le proprie cerchie, in particolare sui loro profili social, *amici di amici* senza valutare attentamente a chi stanno dando accesso alle proprie informazioni, alle proprie foto, spesso ai luoghi che frequentano, a quello che in definitiva viene chiamato *diario virtuale*. Tra le poche accortezze che molti ragazzi utilizzano per valutare l'affidabilità e la sicurezza di chi chiede loro di essere aggiunto tra gli amici, c'è quella di valutare il numero di amici in comune con la persona che aggiungono. Aiutare i propri alunni a tutelarsi, scegliendo con cura chi frequentare *online*, è allora un compito importante anche dell'insegnante che contribuisce in questo modo alla loro tutela nella vita virtuale, con ripercussioni non banali nella vita reale.

Se questo è più in generale lo scenario che vede come protagonisti i nostri ragazzi nella vita di ogni giorno al di fuori delle mura scolastiche, i rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC derivano da un uso non corretto del telefono cellulare personale o dei pc/ tablet della scuola, collegati alla Rete. Il telefono cellulare personale non è richiesto dalla scuola perché non è ritenuto indispensabile in ambito scolastico, ma viene fornito dai genitori degli alunni soprattutto per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari dotati di particolari applicazioni e di collegamento a Internet, oltre che parlare e scrivere messaggi con i genitori, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti non decorosi o violenti, accedere a siti, ascoltare musica e giocare con videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a Internet.

È opportuno che i docenti, nell'espletamento delle proprie funzioni di formatori ed educatori sappiano cogliere ogni opportunità per riflettere insieme agli alunni sui tali rischi. Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la nostra scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Dunque, 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.

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.

È utile, in via preliminare, richiamare anche gli atti persecutori classificabili come ***Bullismo***. Rientrano in tale categoria:

- La sopraffazione fisica, verbale e/o psicologica;
- la violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata;
- l'intenzione di nuocere;
- l'isolamento sociale della vittima.

Rientrano invece tra gli atti persecutori classificabili come ***Cyberbullismo***:

- FLAMING: Litigi nei forum di discussione, con l'uso di un linguaggio violento e volgare
- HARASSMENT: molestie attuate attraverso l'invio ripetuto di messaggi offensivi
- CYBERSTALKING: invio ripetuto di messaggi che includono esplicite minacce fisiche
- DENIGRAZIONE: sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione
- OUTING ESTORTO: registrazione di confidenze per poi inserirle integralmente in un blog pubblico
- TRICKERY: spinta, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete
- IMPERSONATION: insinuazione all'interno dell'account di un'altra persona
- ESCLUSIONE: estromissione intenzionale di una persona da un gruppo online
- HAPPY SLAPPING: ripresa, con il videotelefono, macchina fotografica o videocamera, di scene violente al fine di mostrarle ad amici o di diffonderle sulla rete
- EXPOSURE: pubblicare informazioni private e/o imbarazzanti su un'altra persona
- SEXTING: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.
- PEDOPORNOGRAFIA: 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 gestione dei casi rilevati andrà differenziata a seconda della loro gravità. Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi possono essere affrontati con la convocazione di genitori e alunni, alla presenza del Dirigente scolastico e del Referente del Cyberbullismo, per riflettere insieme sull'accaduto e individuare strategie comuni d'intervento. Nei casi più gravi e in ogni ipotesi di reato, occorre valutare tempestivamente con il Dirigente Scolastico come intervenire, convocando con urgenza i genitori. Tutte le segnalazioni dei docenti devono essere messe a verbale e protocollate.

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, con 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;

Viene sottolineato inoltre come il sistema scolastico debba prevedere *azioni preventive ed educative* e non solo sanzionatorie.

Ogni Istituzione scolastica deve nominare al proprio interno un Referente per le iniziative di prevenzione e contrasto che si assume il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, tale figura può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio. Tale figura potrà svolgere un importante compito di supporto al Dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), di atti e di documenti (PTOF, PdM, Rav).

Sulla base delle *Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo* del gennaio 2021, inoltre, le scuole devono prevedere un Team Antibullismo costituito dal Dirigente scolastico, dal/ dai referente/i per il bullismo – cyberbullismo, dall'animatore digitale e dalle altre professionalità presenti all'interno della scuola (psicologo, pedagogista, operatori socio-sanitari), ed un Team per l'Emergenza: questi hanno la funzione di coadiuvare il Dirigente scolastico, coordinatore dei Teams, nella definizione degli interventi di prevenzione del bullismo e di intervenire nelle situazioni acute di bullismo.

Segnalazione e gestione dei casi – Protocollo attuativo

Segnalazione – Come e a chi

Quando emerge un fatto di *bullismo/cyberbullismo* vanno considerati tutti gli attori in gioco: vittima/e, bullo/i, spettatori o maggioranza silenziosa, aiutanti/sostenitori, difensori del bullo o della vittima, adulti.

⇨ **PROTOCOLLO DI EMERGENZA NEI CASI DI BULLISMO E CYBERBULLISMO (allegato 1)**

⇨ **MODULO DI PRIMA SEGNALAZIONE (Allegato 2)**

Sanzioni disciplinari

I comportamenti accertati che si configurano come forme di *bullismo* e *cyberbullismo* sono considerati come infrazioni gravi e vengono sanzionati sulla base del *Regolamento disciplinare* degli studenti. La sanzione disciplinare, commisurata all'intensità dell'episodio, deve prevedere anche una attività riparatoria ed educativa che sia visibile e vada a beneficio della vittima e/o della classe. La classe a sua volta dovrà fare una sua azione riparatoria nei confronti della vittima. Le sanzioni saranno particolarmente incisive per fatti di estrema gravità, preferibilmente con l'attivazione di percorsi educativi di recupero mediante lo svolgimento di attività di natura sociale, culturale e in generale a vantaggio della comunità scolastica. Vengono considerati deplorevoli e sanzionabili anche le condotte dei compagni sostenitori del bullo.

Attenuanti e aggravanti

- Il riconoscimento dell'errore, il risarcimento del danno e le scuse personali costituiscono attenuanti per le quali si applica la riduzione della pena (sono esclusi i reati di violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata, e il reato di cyberstalking).
- Aver commesso un'infrazione disciplinare, in concorso con una o più persone, costituisce aggravante per la quale si applica l'aumento della sanzione.
- È possibile convertire parte della sanzione nello svolgimento di attività educative, definite in accordo con le famiglie secondo un piano educativo condiviso.

Obbligo di denuncia

Devono essere denunciati dal Dirigente scolastico alle autorità competenti (carabinieri, polizia, polizia postale) i seguenti reati perseguibili d'ufficio:

- rapina ed estorsione (art 628 c.p. e art 629 c.p.) riferibili ad episodi di minacce e violenze per ottenere (o sottrarre) oggetti o somme di denaro;
- lesioni gravissime (art 582 c.p. – 585 c.p.) e lesioni guaribili in più di 40 giorni o che comportano una diminuzione permanente della funzionalità di un organo;
- violenza sessuale (art 609 s.p.) commessa singolarmente o in gruppo – in questo caso viene considerata più grave e punita più severamente (per chiarire cosa si intende per violenza sessuale, bisogna considerare che ogni atto sessuale rientra in questa definizione, ad esempio: se un gruppo di minori blocca fisicamente una compagna palpeggiandola, rispondono tutti penalmente e non solo la persona che materialmente esegue l'atto);
- violenza o minaccia a pubblico ufficiale per alunni che hanno compiuto il quattordicesimo anno di età (art. 336 c.p. e art. 337 c. p.).

Episodi di *bullismo* perseguibili in caso di querela:

- lesioni, percosse, minacce, ingiurie, diffamazione, molestia, atti persecutori/ stalking (art. 582,581, 612, 591, 595 ,660,612 del Codice Penale): in questi casi è necessario informare la famiglia (e/o i Servizi Sociali) che può procedere alla querela, a sua discrezione. Il mancato avviso alla famiglia, da parte dell'Istituzione scolastica, è passibile di denuncia.

Gli attori sul territorio per intervenire

- ***HelpLine***: linea telefonica di ascolto e consulenza, prima risposta ai bisogni di bambini e adolescenti di essere ascoltati, operativa 24 ore su 24;
  Tel. 1.96.96

- ***Polizia Postale***: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
  Sezione *Avellino* - Via Ammiraglio Ronca, 13 – Tel. 0825/21074 - 0825 34103

- ***Comitato Unicef Campania***: svolge un ruolo di difensore dei diritti dell'infanzia
  Telefono: 081 71 470 57
  e-mail: comitato.campania@unicef.it
  Largo Domenico Martuscelli, 26 80127 – Napoli

- ***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.
  Centro Direzionale Isola, F/8
  80143 Napoli
  Tel. Segr. conciliazioni: 081/7783833 – 3835
  Tel. Segr. Co.re.com: 081/7783833 -835
  E-mail: corecom.campania@consiglio.regione.campania.legalmail.it
  Sito Web**:** http://www.consiglio.regione.campania.it/corecom/jsp/index.jsp

- ***Ufficio Scolastico Regionale***: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
  per la *Campania*:Via Ponte della Maddalena,55 80142 Napoli
  Sito web: campania.istruzione.it

- ***Azienda Sanitaria Locale***: fornisce supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche.
  Consultorio psicologico Avellino
  Centro Sociale Samantha della Porta – Via Morelli e Silvati – Avellino – Tel. 0825 21969

- ***Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico***: segnala all'Autorità Giudiziaria e ai Servizi Sociali competenti; accoglie le segnalazioni di presunti abusi e fornisce informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
  Centro Direzionale Is. F/8 - 80143 Napoli
  Tel. 081/7783503 – 3843

- ***Tribunale per i Minorenni***: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.
  Viale Colli Aminei, 42 – 80131 Napoli (NA)
  Tel. 081.7449111
  E-mail: tribmin.napoli@giustizia.it
  Sito: www.tribunaleminorenni.napoli.it/

Diritto all'oblio

E' importante sapere che il *Garante italiano* ha adottato un provvedimento di accoglimento di richieste di rimozione di collegamenti in Rete lesivi di diritti (*Diritto all'oblio*).

Per quanto riguarda Google e la richiesta di rimozione di contenuti lesivi, basta cliccare e compilare il form su:

https://support.google.com/legal/answer/3110420?source=404&visit_id=637335154839186682-742172507&rd=1

La pagina in cui sono presenti i contenuti diffamatori verrà oscurata. Per chiederne la totale cancellazione, bisognerà rivolgersi obbligatoriamente al titolare del sito.

Per segnalare violazioni di legge o l'uso improprio del web molte piattaforme hanno predisposto un link o sono state attivate funzioni specifiche:

- Facebook: www.facebook.com/safety
- Twitter: è stata attivata la funzione *mute* per bloccare gli account non desiderati
- Instagram: il social consente di segnalare immagini e commenti di account non desiderati oltre a keywords attraverso le quali possono essere bloccati i contenuti in cui appaiono le parole scelte.

In caso di richiesta di oscuramento non ottemperata …

Qualora entro le 24h successive al ricevimento dell'istanza il soggetto responsabile non abbia comunicato di aver assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro 48h non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito Internet o del *social media*, l'interessato può rivolgere analoga segnalazione o richiesta, mediante segnalazione o reclamo, al ***Garante per la protezione dei dati personali*** (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6732688) il quale, entro 48h dal ricevimento della richiesta, provvede ai sensi degli artt.143 e 144 del decreto legislativo 30/06/2003 n.196 (Allegato 3).

Si evidenziano anche i servizi messi a disposizione dal ***Safer Internet Center*** per segnalazione di contenuti illegali e dannosi:

Telefono Azzurro: http://www.azzurro.it/emergenza-0
Clicca e segnala di Telefono Azzurro www.azzurro.it/it/clicca-e-segnala
Stop-it di *Save the Children* www.stop-it.it

Allegati

Allegato1 – Protocollo di emergenza in caso di bullismo e cyberbullismo

Allegato 2 – Modulo di prima segnalazione

Allegato 3 – Modulo di segnalazione al Garante per la protezione dei dati personali

Allegato 4 – Vademecum per gli alunni su Uso sicuro del web

Allegato 5 – Consigli ai genitori per un Uso responsabile di Internet a casa