



Istituto di Istruzione Superiore
“VANVITELLI STRACCA ANGELINI”

Via Umberto Trevisani, 4 - 60127 Ancona - Tel. 071 4190711 - Fax 071 4190712
C.F. 93084450423 - Cod. meccanografico ANIS00400L – Sito www.istvas.edu.it
email: anis00400l@istruzione.it - anis00400l@pec.istruzione.it - scuola@istvas.edu.it
Codice univoco fatturazione UF01E9 - Codice IPA: istsc_anis00400l



INDIRIZZI DI STUDIO: Agraria Agroalimentare e Agroindustria - Amministrazione, Finanza e Marketing –Chimica, Materiali e Biotecnologie (Ambientali e Sanitarie) - Costruzioni, Ambiente e Territorio - Sistema Moda

Documento di ePolicy

SAVORE FRANCESCO

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.

Essa autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati nell'uso e nella navigazione in rete.

L'Istituto Vanvitelli Stracca Angelini, consapevole dei problemi che possono derivare da un uso scorretto ed incauto della rete si attiva per attuare attività di prevenzione, controllo e formazione di studentesse, studenti e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come veri e propri reati.

La scuola opera in stretto collegamento con le forze dell'ordine, come la Polizia Postale Telematica, con la Procura della Repubblica, con istituzioni del settore educativo ed Enti Locali, per mettere in campo strategie di prevenzione e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

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.

Dirigente Scolastico

È responsabile della presentazione di questo documento all'attenzione del Collegio dei Docenti e all'approvazione del Consiglio di Istituto; deve anche valutare l'efficacia delle azioni intraprese e monitorarne l'attuazione, anche in collaborazione con personale scolastico, enti locali e referenti territoriali.

A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal

personale ATA che ne vengano a conoscenza.

Animatore digitale

Cura la redazione iniziale e l'eventuale revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/personale ATA, genitori e studenti), mediante pubblicazione sul sito della scuola. Si relaziona con l'Ufficio Tecnico e l'Amministratore di rete per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Referenti Bullismo e Cyberbullismo

Hanno il compito di coordinare le iniziative di prevenzione e contrasto del bullismo e del cyberbullismo. A tal fine, i referenti di istituto possono avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Personale docente con particolare riferimento ai Coordinatori dei Consigli di Classe

Gli insegnanti sono tenuti a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore Digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- integrare i problemi di sicurezza informatica in tutti gli aspetti del curriculum di studi e in altre attività extracurricolari;
- far comprendere alla componente studentesca e far mettere in pratica le regole

- di comportamento relative alla sicurezza informatica;
- far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
 - controllare l'uso delle tecnologie digitali, smartphone, dispositivi mobili, ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
 - guidare la navigazione di alunni/alunne nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

Personale ATA

Il personale ATA è tenuto a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- controllare la presenza dell'accettazione della liberatoria ai fini della pubblicazione di foto, video degli alunni (personale della segreteria didattica) e comunicare all'Amministratore di rete l'eventuale non accettazione.

Componente studentesca

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy.

In particolare sono tenuti a:

- non utilizzare dispositivi personali (smartphone, dispositivi mobili, ecc.) durante le attività didattiche se non espressamente consentito dal personale docente. Tale utilizzo deve rispondere a quanto previsto nel regolamento di Istituto, nel presente documento e nella normativa vigente;
- avere una buona comprensione delle possibilità di ricerca sul web e della

necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali e conoscere gli elementi essenziali della Netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o email);

- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati informando tempestivamente il coordinatore di classe;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare la rete Internet in modo appropriato.

La scuola coglierà ogni occasione per sensibilizzare i genitori su questi problemi attraverso: incontri con la Polizia Postale ed altri esperti o educatori; pubblicazione di circolari; comunicazioni ed eventuali approfondimenti sul sito della scuola dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di eSafety e a seguire le linee guida sull'uso appropriato di:

- immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- sezioni del sito della scuola dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli nella scuola.

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).

da compilare con le indicazioni contenute nella lezione

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/le 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.

da compilare con le indicazioni contenute nella lezione

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.

Le infrazioni alla policy possono essere rilevate da docenti e personale ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti e personale ATA.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che, nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361 del codice penale). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- Minaccia: in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale);
- Induzione alla prostituzione minorile (art. 600 bis);
- Pedopornografia (art. 600 ter);
- Corruzione di minorenni (art. 609 quinquies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione. La realizzazione di quanto esposto è supportata dalla partecipazione dell'Istituto al

progetto di Educazione alla legalità.

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 presente policy è allegata in appendice al Regolamento di Istituto.

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.

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola del presente documento, si prevedono le seguenti azioni:

discussione collegiale sui contenuti, sulle pratiche indicate, per il corpo docente e il personale ATA (nelle sedi competenti);

- eventuale revisione, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente a seguito di segnalazioni ricevute dalle varie componenti; discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime, per la componente studentesca;
- inserimento di un estratto di questo documento nel vademecum dello studente
- organizzazione di incontri di sensibilizzazione sul tema della sicurezza

informatica e di informazione circa i comportamenti da monitorare o da evitare, per i genitori.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare eventi e/o forum di discussione di presentazione e conoscenza dell'ePolicy rivolto a studenti, docenti e personale ATA

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per il monitoraggio e l'aggiornamento dell'ePolicy.
- Promuovere incontri formativi per gli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- promuovere la partecipazione di un gruppo rappresentativo di genitori sui temi dell'e-policy.

Capitolo 2 - Formazione e curriculum

2.1. Curriculum 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.

Ciascun Consiglio di Classe avrà cura di strutturare il proprio piano di lavoro in modo da agevolare negli studenti l’acquisizione di competenze digitali.

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.

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.

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta da docenti dell'Istituto che fanno parte del team digitale, per cui il MIUR prevede opportuni percorsi rispettando le esigenze emerse dalla componente Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni.

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.

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale e organizzare incontri formativi dedicati allo scopo.

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.

Si fa riferimento a tutto quanto previsto dal "Codice in materia di protezione dei dati personali, recante disposizioni previste dal Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, dal D.lgs. 101/2018 e s.m.i"

In linea generale, tutti i dati propri e di terzi, di cui i soggetti del presente disciplinare vengono a conoscenza, nell'ambito delle proprie attività, sono da considerarsi riservati e non devono essere comunicati o diffusi a nessuno (anche una volta interrotto il rapporto) salvo specifica autorizzazione esplicita dell'Istituto.

Sia il titolare dei dati, sia i vari soggetti coinvolti dalla presente policy, devono mettere in atto misure tecniche e organizzative adeguate per:

- garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento, nelle modalità necessarie per il loro corretto utilizzo,
- garantire, con tutti i suoi mezzi a propria disposizione, che non siano resi accessibili dati personali ad un numero indefinito di persone fisiche.

La progressiva diffusione delle nuove tecnologie espone l'Istituto ed i soggetti che hanno contatti con esso a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto scolastico e di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'Istituto sottolinea l'importanza di intraprendere, da parte di tutti, azioni tese a difendere con ogni mezzo possibile ed a gestire nelle modalità idonee, i dati ottenuti.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

L'Istituto a conoscenza di tali rischi mette a disposizione, oltre che supporti e credenziali informatiche necessari per lo svolgimento delle proprie finalità istituzionali, anche un numero di telefono o una e-mail della scuola personale i contatti tra componente studentesca o genitori.

Tali strumenti ed informazioni dovranno essere utilizzati solo ed esclusivamente per gli scopi istituzionali ed i loro utilizzatori dovranno tutelarne il contenuto e la riservatezza.

All'atto dell'iscrizione e/o inizio di un rapporto lavorativo con l'Istituto è richiesto, ai vari soggetti, di firmare una informativa scritta per consentire l'uso, ai fini istituzionali, dei propri dati personali.

Per ogni altro caso non previsto dall'informativa precedente, compresa quella relativa all'utilizzo di immagini e video delle/dei minori, verrà richiesto il consenso con una informativa apposita.

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'Istituto attualmente è dotato di una rete wireless destinata all'utilizzo didattico da parte del corpo docente, realizzata grazie ai contributi ottenuti dall'accettazione del progetto PON 9035 del 13/07/2015 - FESR - realizzazione/ampliamento rete LanWLAN. La scuola abilita l'accesso alla rete previo reperimento del MAC address (detto anche indirizzo fisico) dei dispositivi personali e consegna di una password unica a livello di Istituto allo scopo di estendere il servizio e permettere al personale in oggetto di accedere a contenuti e materiali in rete e permettere l'applicazione di una didattica innovativa e più coinvolgente per gli studenti ad essi affidati. Al contrario per gli alunni l'accesso alla rete internet, utilizzando la rete cablata, è permesso nei laboratori, nelle aule digitali e negli spazi adibiti attraverso l'abilitazione all'accesso tramite l'account personale. Tale modalità ha lo scopo di monitorare meglio eventuali usi impropri e utilizzare in maniera efficace e consapevole i contenuti della rete per utenti che ancora non hanno acquisito la maturità psicologica per valutare gli effetti negativi che azioni non consone possono provocare.

Ciascun utente connesso alla rete dovrà rispettare il presente regolamento e la legislazione vigente, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta Netiquette.

La componente studentesca e tutto il personale, dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

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.

E-mail

L'Istituto fornisce una casella di posta elettronica "utente@istvas.it" a tutto il personale docente, personale ATA e alla componente studentesca. Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo. Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola, per consentire l'attivazione di protocolli di controllo. E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

Sito web della scuola.

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, organigramma della scuola, organigramma della sicurezza, albo online ed amministrazione trasparente. Il sito web non permette interazione con l'utenza.

La scuola fa uso anche di un sito specifico per la pubblicazione del piano dell'offerta formativa finalizzato alle attività di orientamento scolastico delle classi di scuola secondaria di 1° grado.

Anche questo sito non permette l'interazione con l'utenza.

Social network.

La scuola nella pratica didattica cerca di educare la componente studentesca all'uso sicuro dei social network. Per esempio a ogni utente è consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione. La componente studentesca non deve pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico.

Registro elettronico.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente registra assenze, valutazioni, note e osservazioni.

L'uso del registro elettronico è spiegato nel manuale pubblicato sul sito della scuola. Coloro che non possono accedere ad Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe o direttamente al personale della segreteria.

Piattaforma “Google Workspace for Education” per la didattica digitale integrata.

La G Workspace for Education è un insieme di applicazioni web dedicate alla comunicazione e alla collaborazione in ambiente scolastico e universitario di cui, grazie ad un accordo con Google, è possibile usufruire gratuitamente.

La G Workspace for Education è attualmente la piattaforma più utilizzata nelle scuole italiane e il suo impiego nelle istituzioni scolastiche è sostenuto dal Ministero dell'Istruzione.

La G Workspace for Education ha diverse applicazioni, tra cui le più utilizzate sono:

- Gmail
- Google Moduli
- Google Presentazioni
- Google Fogli
- Google Documenti
- Drive
- Calendar
- Chat
- Meet
- Classroom

L'utilizzo della piattaforma di Google offre i seguenti vantaggi:

- sicurezza e rispetto della Privacy
- fruibilità e accessibilità da qualsiasi dispositivo on line (pc, tablet, smartphone), in qualsiasi parte del mondo
- risparmio economico (la piattaforma è gratuita)
- spazio di archiviazione di 30 GB per ogni account
- semplicità ed immediatezza operativa grazie all'ambiente di lavoro familiare (interfaccia grafica Google)

Ad ogni studente/studentessa verrà assegnato un account personale (cognome.nome@istvas.it).

L'account permette l'utilizzo delle app della piattaforma di Google sopraindicate, in particolare: - la app Drive offre la possibilità di accedere alle condivisioni online di file e documentazione didattica.

- la app Calendar permette di gestire gli impegni personali e condivisi con i docenti
- la app Gmail è utilizzabile per comunicare all'interno dell'Istituto, con altri alunni e con i docenti, a scopo didattico, ed è anche disponibile per comunicazioni esterne alla scuola. la app Meet è utilizzata per le lezioni in DID e per le riunioni video. Questa app può essere utilizzata solo all'interno del dominio@istvas.it, realizzando così una modalità d'uso sicura e rispettosa della privacy.

Alle famiglie degli studenti minorenni è richiesto inoltre un impegno fattivo di collaborazione con i docenti nel responsabilizzare i ragazzi sulle modalità di accesso a internet e sulle regole a cui attenersi.

La piattaforma di Google presenta diversi livelli di sicurezza dati e tutela della Privacy. In particolare, Google integra la sua Normativa in materia con una serie di norme aggiuntive volte a garantire una maggiore protezione all'interno dell'ambiente education, quali:

- Limitazioni sulla pubblicità. All'interno dei Servizi principali della piattaforma di Google, i prodotti e i servizi Google NON possono contenere annunci pubblicitari. Per gli utenti di G Workspace for Education delle scuole primarie e secondarie, Google non utilizza alcuna informazione personale (o associata a un account Google) per definire il target degli annunci.
- Creazione di account da parte dell'amministratore. L'account G Workspace for Education di uno studente è un account Google creato dall'amministratore del dominio dell'istituto scolastico. Durante la creazione dell'account, l'amministratore può fornire alcuni dati personali dell'utente quali, ad esempio, nome, cognome. Google associa tali dati all'account.
- Proprietà intellettuale. Google non acquisisce la proprietà dei dati degli studenti e dei docenti. Tali dati rimangono di proprietà della scuola. Pertanto, nel momento in cui l'istituzione scolastica decide di interrompere l'utilizzo della piattaforma di Google, i dati vengono restituiti alla scuola stessa.

- Cessione dati. I dati sono di proprietà delle scuole che utilizzano la piattaforma di Google ed è responsabilità di Google proteggerli. Google non cede/ vende a terze parti i dati degli studenti/ docenti, e non condivide con terze parti le informazioni personali presenti nei sistemi, tranne che in rari e circostanziate eccezioni, ad esempio quando è l'utente (solo se maggiorenne) a chiedere di condividerli o se costituisce obbligo di legge.

Infine è opportuno ricordare che la piattaforma di Google è un ambiente di archiviazione e condivisione risorse e rispetta quando indicato e suggerito dal Garante della Privacy in ambito scolastico, come illustrato nel documento "La scuola a prova di privacy".

Ulteriori informazioni sono disponibili a questo indirizzo: <https://edu.google.com/why-google/privacy-security/>

LINK UTILI

Google mette a disposizione guide e supporto per gli utenti tramite l'help in linea, consultabile all'indirizzo: <https://support.google.com/>

Normativa Google in materia di sicurezza dei dati e tutela della Privacy: <https://www.google.com/intl/it/policies/privacy/>

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 la componente studentesca.

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente. Individui con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili. Ogni altro utilizzo costituisce infrazione, per tutte le disposizioni al riguardo si fa riferimento all' "Allegato n.1 del Regolamento (uso dei cellulari ed altri dispositivi)" pubblicato sul sito della scuola.

Per il personale docente e ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.

Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate. L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione. Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Il nostro piano d'azioni

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

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali 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.

Le misure di prevenzione comprendono l'integrazione nel curriculum dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe. Si demanda agli indirizzi disciplinari la scelta dei settori su cui focalizzare la formazione: a titolo di esempio il

dipartimento letterario si può soffermare in particolare sugli aspetti legati all'affettività, alla socializzazione e alla cittadinanza, quello tecnologico-scientifico-matematico sulle questioni tecniche e legate alla salute, quello di arte/musica sulla tutela del diritto d'autore. La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento. Il nostro Istituto attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyberbullismo. La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che studentesse e studenti alunni vivono: si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. I Docenti, in particolare, sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti. La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

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).

Da implementare con le indicazioni contenute nella lezione.

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.

Da implementare con le indicazioni contenute nella lezione.

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?

Da implementare con le indicazioni contenute nella lezione.

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 medialmente 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.

Da implementare con le indicazioni contenute nella lezione.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi 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.

Da implementare con le indicazioni contenute nella lezione.

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](#).

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

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

Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

Organizzare uno o più incontri anche durante attività assembleari per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.

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 minorenni 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 analogha 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.

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che studentesse e studenti alunni vivono. La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

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).

Per la segnalazione è possibile usare la scheda di segnalazione da inviare direttamente al Dirigente Scolastico o al referente e-policy o ai referenti Bullismo/Cyberbullismo

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, l'Istituto prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- Email del Dirigente Scolastico o del referente e-policy o del referente Bullismo Cyberbullismo;
- sportello di ascolto CIC;
- progetti specifici (psicologo scolastico) e sportello di ascolto relativo
- docenti referente per Bullismo/Cyberbullismo

Per ogni altra indicazione si faccia riferimento al "REGOLAMENTO PER LA PREVENZIONE E IL CONTRASTO AL BULLISMO E AL CYBERBULLISMO" deliberato dal consiglio di istituto dell'IIS Vanvitelli Stracca Angelini di Ancona

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.

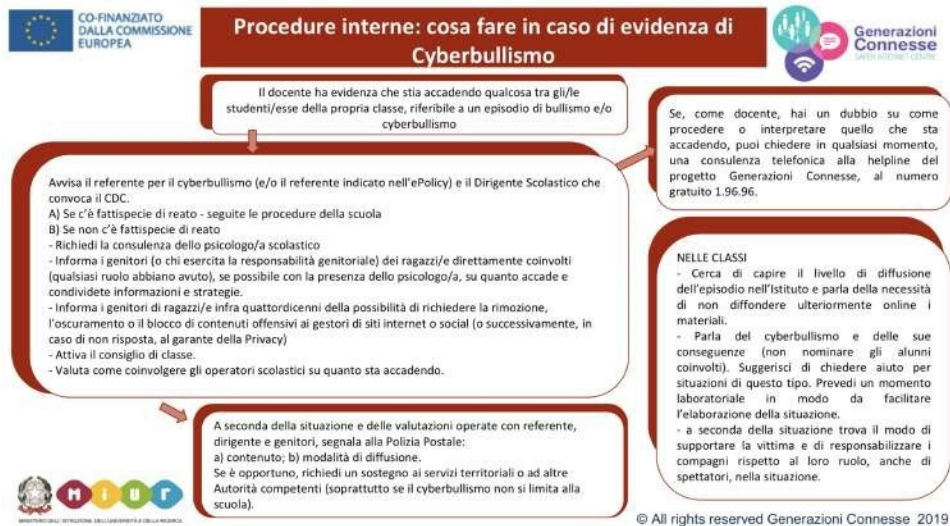
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza 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.

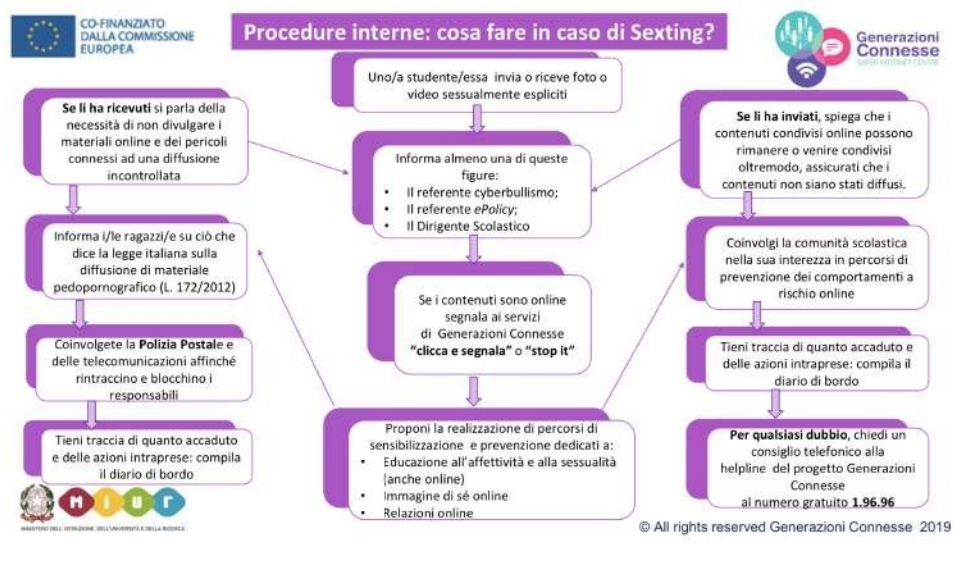
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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; raccolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

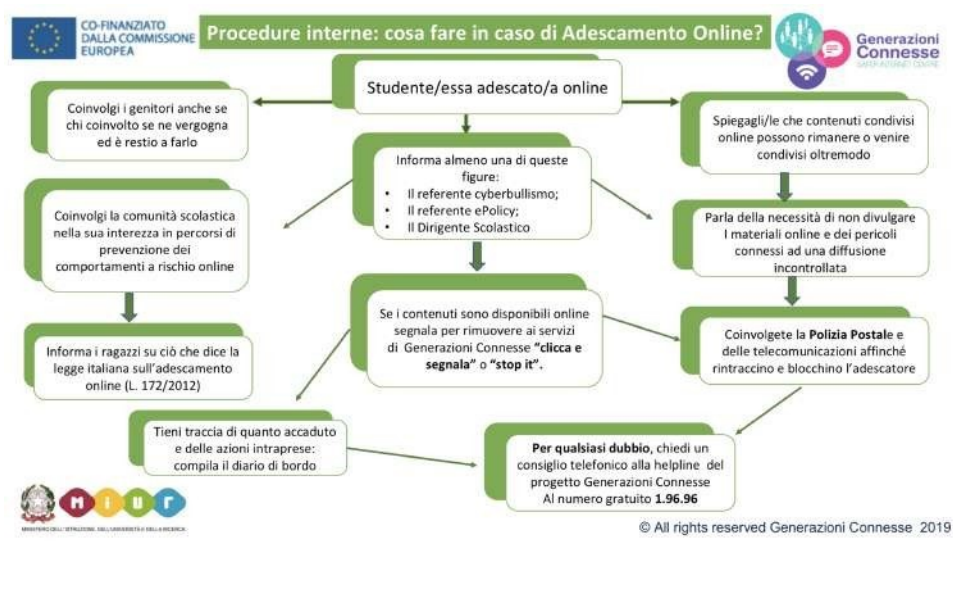
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



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](#)

Il nostro piano d'azioni

Non è prevista nessuna azione.

