

I.C. "DE FILIPPO-DE RUGGIERO"  
BRUSCIANO (NA)  
Prot. 0000839 del 10/03/2023  
I (Uscita)

a.s. 2022-23

# Documento di e-Policy

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA  
ON LINE

NAIC8EK00N

IC De Filippo De Ruggiero

via V. Veneto

80031 - BRUSCIANO



## Capitolo 1 - Introduzione al documento di 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'e-Policy*
  - 1) *Scopo dell'e-Policy*
  - 2) *Ruoli e responsabilità*
  - 3) *Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto*
  - 4) *Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica*
  - 5) *Gestione delle infrazioni alla e-Policy*
  - 6) *Integrazione con regolamenti esistenti*
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*
  - 7) *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*
  - 8) *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*
  - 9) *Pedopornografia*
5. *Segnalazione e gestione dei casi*
  - 1) *Cosa segnalare*
  - 2) *Come segnalare*
  - 3) *Gli attori sul territorio per intervenire*
  - 4) *Allegati con le procedure*

# Capitolo 1- Presentazione dell'e-Policy

## 1.1 Scopo dell'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.

La e-Safety Policy stabilisce i principi fondamentali per l'utilizzo delle tecnologie e per l'uso responsabile di Internet per tutta la comunità scolastica.

## 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 esso.

Il ruolo del Dirigente scolastico è quello di:

- garantire la sicurezza, tra cui la sicurezza on-line, dei membri della comunità scolastica;
- garantire agli insegnanti una formazione adeguata per un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- supervisionare sul ruolo di tutte le figure educative all'interno dell'istituzione scolastica.

Il ruolo del Direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta ad un uso improprio o a dannosi attacchi esterni;
- garantire 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.

Il ruolo dell'Animatore digitale, delle Figure strumentali tecnologia e del Team Digitale è quello di fornire supporto e sostegno al lavoro dei docenti, in particolare all'uso delle TIC, e nella didattica devono:

- stimolare la formazione interna riguardo ai rischi on-line e alle misure di prevenzione e gestione degli stessi;

- *monitorare e rilevare le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola;*
- *assicurare l'accesso alla rete della scuola solo tramite password; curare la manutenzione e lo sviluppo del sito web della scuola, in autonomia operativa o attraverso consulenti esterni;*
- *coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".*

*Il compito dei Docenti è quello di:*

- *informarsi/aggiornarsi sull'uso sicuro delle tecnologie digitali e di Internet;*
- *integrare l'utilizzo corretto e sicuro delle TIC e di Internet nel curriculum di studio e nelle attività didattiche ed educative; presentare agli alunni le potenzialità delle TIC per la ricerca di contenuti e materiali, evitando il plagio e rispettando i diritti d'autore; assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;*
- *controllare 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, guidare gli alunni a siti controllati e verificati come adatti per il loro uso;*
- *comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;*
- *segnalare 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.*

*Disciplina dei docenti:*

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

- *un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;*
- *un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;*
- *un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;*
- *una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;*
- *una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;*
- *una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;*
- *una registrazione della videolezione in cui sono visibili i volti degli alunni.*

Le procedure, in questi casi, sono quelle previste dalla legge e dai contratti di lavoro. Gli Alunni sono chiamati, in generale, in accordo con le indicazioni inserite nel Patto di corresponsabilità, a:

- usare le tecnologie secondo le indicazioni dei docenti e mai con iniziative personali;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line;
- rispettare gli altri anche quando si comunica in rete.

#### Disciplina degli alunni:

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a Scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- un uso della rete e delle risorse tecnologiche e digitali per la DID per offendere, giudicare, infastidire o impedire a qualcuno di esprimere il proprio pensiero;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti; il collegamento a siti web non indicati dai docenti
- la condivisione della piattaforma di didattica a distanza con terzi;
- la diffusione in rete delle attività realizzate dal docente, con il docente e i compagni;
- la diffusione in rete di registrazioni, fotografie e screenshot relativi alle attività di didattica a distanza;
- la diffusione di registrazioni o foto relative alle persone presenti in una videolezione.

#### Sono previsti interventi:

- di carattere educativo
- di rinforzo dei comportamenti corretti e riparativi dei disagi causati,
- di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe,
- di prevenzione e gestione positiva dei conflitti,
- di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà
- di promozione della conoscenza e della gestione delle emozioni.

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

#### Disciplina dei genitori:

I Genitori, in accordo con le indicazioni inserite nel Patto di corresponsabilità, devono:

- sostenere la linea di condotta della Scuola nei confronti dell'utilizzo delle tecnologie;
- seguire gli alunni nello studio a casa, adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllando l'utilizzo del pc e di Internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in caso di un uso non responsabile o pericoloso delle tecnologie digitali o di Internet

### **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).*

### **1.4 Condivisione e comunicazione dell'e-Policy 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.*

### **1.5 Gestione delle infrazioni alla e-Policy**

*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.*

*La scuola:*

- *Prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line.*

- *Procederà a dare informazioni sulle infrazioni e sulle eventuali sanzioni.*
- *Tratterà eventuali denunce di bullismo e cyberbullismo in conformità con le leggi vigenti.*

## **1.6 Integrazione dell'e-Policy 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.*

*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, ottenuto tramite la somministrazione di questionari, sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.*

*Dalle risposte si è determinato che:*

- 1. Il corpo docente possiede conoscenze specifiche sulle TIC (anche derivante da corsi di formazione organizzati dalla scuola) e le utilizza nella didattica.*
- 2. Il corpo docente utilizza i pacchetti di scrittura, calcolo e presentazioni, producendo materiale cartaceo di supporto alle attività didattiche.*
- 3. Il corpo docente utilizza con frequenza la LIM. Oltre alla proiezione video e alle presentazioni, vengono utilizzate specifiche risorse didattiche digitali (ad es. software didattici).*
- 4. Il corpo docente prevede, in maniera continuativa, lo svolgimento a scuola di attività di ricerca ed elaborazione dei contenuti che si avvalgono di fonti online. Sono previste attività specifiche di formazione sull'utilizzo critico delle fonti online e sulla rielaborazione dei contenuti. Il carattere delle lezioni favorisce la partecipazione attiva degli studenti/studentesse.*
- 5. Di recente, non sono stati sostenuti corsi di aggiornamento in merito all'utilizzo sicuro e positivo di internet da parte dei docenti.*
- 6. Sono stati organizzati eventi ai quali una piccola parte della comunità scolastica di docenti, studenti/studentesse e genitori ha preso attivamente parte, collaborando e cercando di sensibilizzare il resto della comunità rispetto alle tematiche della partecipazione attiva oggetto delle iniziative in essere.*
- 7. La scuola organizza incontri o seminari aperti agli studenti/studentesse, ai quali una piccola parte risponde con interesse attivo, promuovere il rispetto delle diversità tramite attività programmate, specifiche e/o trasversali.*
- 8. È attivo uno sportello di ascolto. La scuola promuove, non solo la conoscenza, ma anche l'utilizzo del servizio, la cui attività è nota alla totalità della comunità scolastica.*
- 9. La scuola è dotata di un Regolamento di Istituto.*
- 10. La scuola è dotata di rete Wi-Fi, scolastica, regolata da password accessibile agli studenti/studentesse solo in momenti particolari previsti da attività didattiche. È prevista una supervisione delle attività degli studenti/studentesse da parte del personale docente.*



11. Sono state previste attività curriculari ed extracurriculari finalizzate alla prevenzione dai rischi di Internet e delle tecnologie digitali.
12. La scuola ritiene importante sviluppare le competenze digitali dei propri studenti/studentesse, per cui ha predisposto percorsi curriculari specifici nell'ambito delle attività di Cittadinanza e Costituzione.
13. La scuola ritiene utile la definizione di una Policy di e-safety, ed ha attivato un percorso per una sua definizione ed attuazione
14. La scuola dispone di una procedura standardizzata e definita per la rilevazione e il monitoraggio degli episodi problematici correlati all'utilizzo di internet e delle tecnologie digitali.
15. Eventuali episodi rilevati sono segnalati dai docenti alla Dirigenza Scolastica per la loro gestione, e vengono gestiti a seconda dei casi seguendo prassi interne consolidate.
16. Esistono prassi informali, costruite nel tempo, con le autorità competenti e con i servizi socio-sanitari del territorio per la gestione condivisa del caso.
17. Il personale scolastico conosce, comprende e usa regolarmente la procedura di segnalazione, monitoraggio e gestione di incidenti e abusi online. Si sta avviando ad una specifica Policy di e-safety che supporterà i docenti in caso di problematiche (maltrattamenti e/o abusi) riferite agli studenti/studentesse.
18. Il corpo docente conosce le linee generali del PNSD.

Successivamente, grazie al percorso guidato e al materiale di supporto fornito dalla piattaforma, sono stati individuati i punti di forza e di debolezza della scuola:

#### **PUNTI DI FORZA**

1. Aule dotate di LIM e computer
2. Esistenza di laboratori informatici e di lingua.
3. Fibra per la connessione ad internet
4. La coscienza da parte dei docenti di doversi mettere in gioco e la disponibilità a confrontarsi in modo critico e consapevole con l'innovazione.
5. Il desiderio dei docenti di partecipare a corsi di formazione.

#### **PUNTI DI DEBOLEZZA**

1. Miglioramento della manutenzione della dotazione tecnica e l'aggiornamento dei software di computer ed altri hardware.
2. La mancanza della consapevolezza da parte della maggior parte delle famiglie e di conseguenza dei ragazzi delle conseguenze di un cattivo uso di Internet.
3. Formazione dei docenti in merito alla segnalazione e gestione delle problematiche inerenti al cattivo uso di Internet.
4. Collaborazione tra famiglie, studenti e docenti volta a descrivere una nuova visione del fenomeno della rete, le norme comportamentali e le misure per la prevenzione di rischi connessi ad un uso non consapevole delle tecnologie digitali

## 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.*

*La progettazione ed elaborazione del nuovo Curriculum avverrà in continuità con gli obiettivi formativi prioritari indicati nel PTOF 2022/25.*

*Competenza digitale significa utilizzare le nuove tecnologie in autonomia e con responsabilità nel rispetto degli altri e sapendone prevenire ed evitare i pericoli.*

*La Scuola si propone di favorire lo sviluppo di competenze tra cui:*

- *saper valutare e verificare le informazioni on line;*
- *conoscere i rischi relativi all’uso delle tecnologie e di Internet; saper mantenere le informazioni personali private;*
- *saper segnalare eventuali abusi, tra cui il bullismo on-line, e chiedere aiuto ai docenti e ai genitori.*

### 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.*

*A tal proposito l’IC De Filippo-De Ruggiero ha previsto:*

- *individuazione di un Animatore Digitale;*
- *formazione dei docenti in materia di digitale e di didattica attiva con le TIC;*

- *ricognizione e messa a punto delle dotazioni digitali;*
- *monitoraggio della didattica attiva con le TIC come si evince dal PTOF e dei risultati conseguiti.*

*Sono previsti inoltre:*

- *incontri con esperti (Associazioni, psicologi);*
- *materiali informativi tratti dal sito ministeriale Generazioni Connesse per l'approfondimento personale e per le attività con gli studenti.*

## **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.*

*L'IC De Filippo- De Ruggiero realizza inoltre attività di informazione/formazione coerentemente con il Piano Triennale di Istituto su:*

- *uso consapevole dei dispositivi personali per la didattica, uso consapevole delle risorse della rete d'Istituto*
- *utilizzo della piattaforma e-learning Cisco Webex*
- *necessità rilevate ad inizio anno sulla base di una rilevazione bisogni formativi docenti.*

## **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'e-Policy 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.*

*L'IC De Filippo- De Ruggiero promuove il coinvolgimento delle famiglie attraverso:*

- *eventi ed iniziative in accordo con il Consiglio d'Istituto;*
- *materiali di approfondimento per le famiglie (pdf e video) tratti dal sito;*
- *materiale ministeriale Generazioni Connesse inviati tramite il registro elettronico dell'IC De Filippo- De Ruggiero.*

*Il nostro piano d'azioni:*

*AZIONI (da sviluppare in modo sistematico)*

- *Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.*
- *Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.*
- *Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.*
- *Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.*

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

- *Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.*
- *Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.*
- *Organizzare incontri con esperti per i docenti sulle competenze digitali.*

## 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”.*

*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. del 10 agosto 2018, n. 101, entrato in vigore il 19 settembre 2018.*

*In questo paragrafo dell'e-Policy 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 provvede a fornire di volta in volta e in relazione ai diversi progetti le informative e i modelli di liberatoria, conformi alla normativa vigente, da utilizzare in materia di protezione dei dati personali.*

*Il personale scolastico è “incaricato del trattamento” dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie allo svolgimento della propria funzione.*

*I docenti avranno cura, all'atto della consegna delle credenziali, di spiegare agli studenti l'importanza della segretezza della loro password personale e le conseguenze in caso di violazione degli account personali.*

*La Funzione strumentale insieme al team Digitale avrà cura di verificare periodicamente che gli studenti abbiano modificato la password provvisoria assegnata per effettuare il primo accesso.*

### 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.*

### **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.*

*I docenti al momento della presa di servizio presso l'IC De Filippo-De Ruggiero avranno un proprio account personale; inoltre, come concordato in Collegio, possono usufruire della piattaforma di e-learning Cisco webex. Gli account sono strettamente personali, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Questi spazi sono destinati alla ricezione di comunicazioni, alla formazione docenti, all'invio di documentazione e alla condivisione di materiali con gli altri docenti e con gli studenti dell'IC De Filippo-De Ruggiero.*

### 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 e-Policy 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.*

*Responsabile del trattamento dati è il Dirigente scolastico. La gestione del sito stesso è affidata a computer lab di Giovanni Notaro.*

## 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 sé 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.*

*La Scuola mira a promuovere un ambiente di apprendimento sereno, sicuro e accogliente, che insegni ad interagire in maniera responsabile e mette in atto tutte le azioni possibili per contrastare comportamenti di bullismo, cyberbullismo, violenza e prepotenza.*

### 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.*

*Viene nominato un 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).*

*La Scuola avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web. In modo particolare riguardo al Cyberbullismo, al rischio di adescamento online, di Sexting, di entrare in canali di Pornografia e Pedopornografia. Metterà in atto misure informative circa le dipendenze, come la dipendenza da Gioco d'azzardo e da Internet.*

*In particolare, la scuola e i docenti dell'IC De Filippo- De Ruggiero si impegneranno a promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR a implementare la e-Safety Policy con il contributo di tutte le componenti (docenti, studenti, famiglie, personale A.T.A.). Oltre alla nomina di un Referente per le iniziative di prevenzione e contrasto verrà creato un gruppo di lavoro che avrà il compito di rilevare, segnalare, monitorare e quando possibile contrastare questi fenomeni.*

### **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:*

- 1) Apertura di uno sportello di ascolto per docenti, studenti e genitori.
- 2) Il Referente e il gruppo di lavoro costituito da docenti in accordo con il Team del Digitale e l'Animatore Digitale si adopereranno per la segnalazione, il monitoraggio degli episodi e degli attori coinvolti.
- 3) Segnalazione tempestiva dei casi da parte dei docenti al gruppo di lavoro che valuterà la necessità di progettare e costituire percorsi appositi per studenti e docenti in modo da contenere, contrastare ed infine prevenire il fenomeno.

## 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.

Il Referente e il un gruppo di lavoro costituito da Docenti della scuola in accordo con il Team del Digitale e l'Animatore Digitale si adopereranno per la segnalazione, il monitoraggio degli episodi e degli attori coinvolti.

L'istituto è intenzionato, nel prossimo triennio a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale.

## 4.5 Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/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.

Nel prossimo triennio la Scuola si propone di mettere in campo azioni atte a:

- prevenire le conseguenze psicologiche relative al sexting, aiutare i genitori a comprendere quali sono le conseguenze psicologiche e legali del sexting;
- supportare situazioni particolarmente gravi (isolamento sociale, bullismo, depressione, mancanza di fiducia, pensieri di suicidio);
- prevenire i rischi correlati al sexting.

## 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.

- 1) Apertura di uno sportello di ascolto per docenti, studenti e genitori.
- 2) Creazione di un gruppo di lavoro costituito da Docenti della scuola in accordo con il Team Digitale e l'Animatore Digitale per la segnalazione, il monitoraggio degli episodi e degli attori coinvolti.
- 3) Segnalazione tempestiva dei casi da parte dei docenti al gruppo di lavoro che valuterà la necessità di progettare e costituire percorsi appositi per studenti e docenti in modo da contenere, contrastare ed infine prevenire il fenomeno.

## 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](http://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.*

*Il Referente e il gruppo di lavoro costituito da Docenti della scuola in accordo con il Team Digitale e l’Animatore Digitale cercheranno di lavorare per la segnalazione, il monitoraggio degli episodi e degli attori coinvolti nei limiti delle possibilità e delle informazioni ricevute.*

## 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'e-Policy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse.*

*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.*

*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, 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/lle 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 minore e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Help line 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.

Le tipologie più comuni di comportamenti da segnalare sono:

- Uso di dispositivi elettronici per chiamate o messaggi o per altro uso non consentito (giochi, musica, chat, etc.);
- Uso del cellulare per effettuare riprese audio, foto, video;
- Uso del cellulare per diffondere a terzi, in modo non autorizzato, audio, foto o video in violazione delle norme sulla privacy.

## 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 Help line del progetto Generazioni Connesse, al numero gratuito 1.96.96. Per segnalare i casi e tenere traccia di ciò che è avvenuto la scuola utilizza le linee guida di Generazioni Connesse.

L'animatore e il Team Digitale, il Referente, il gruppo di lavoro per il contrasto dei fenomeni sopra descritti rimangono sempre a disposizione dei docenti, del personale Ata e degli alunni per affrontare i singoli casi.

## **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”, senza dimenticare che la Help line di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

**Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

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

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

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

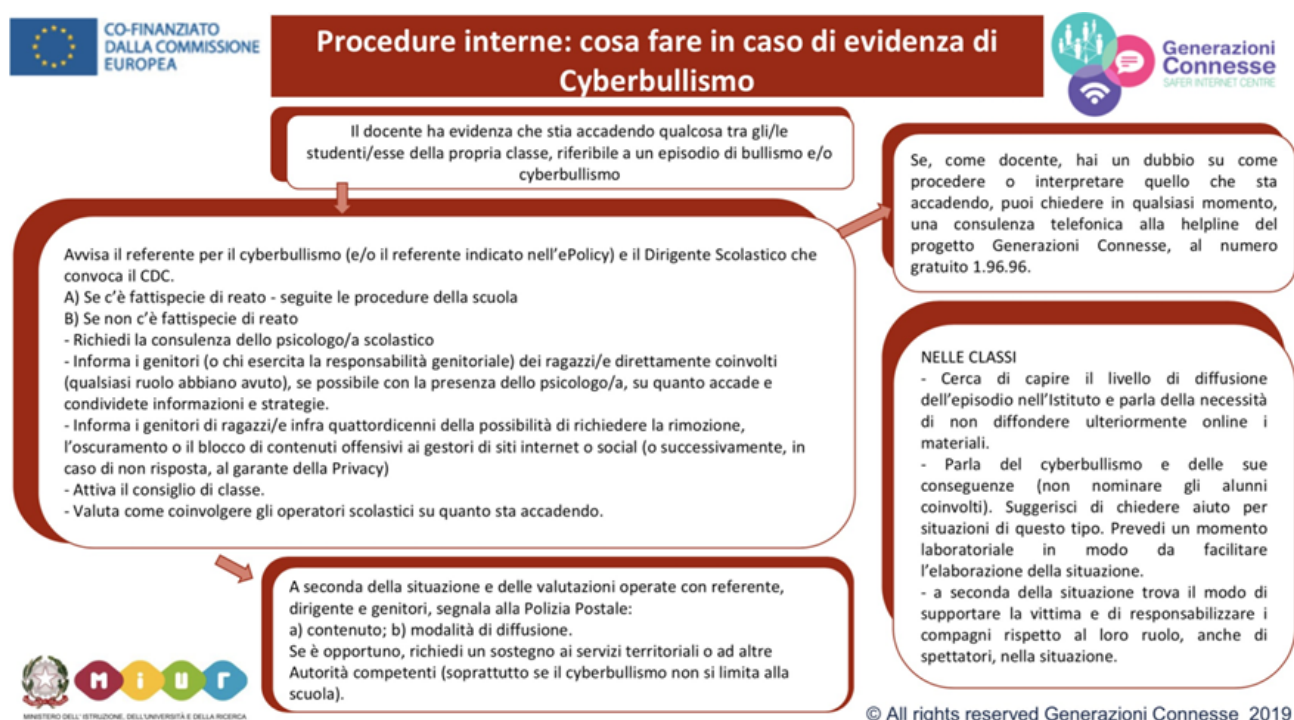
**Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni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

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

**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

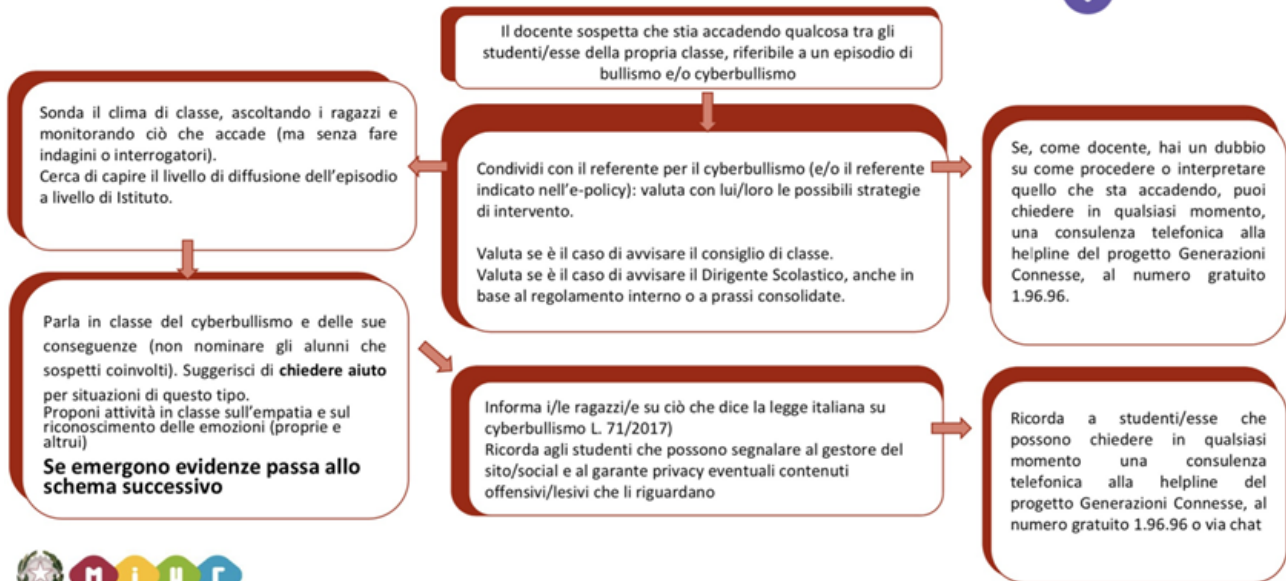
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?







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

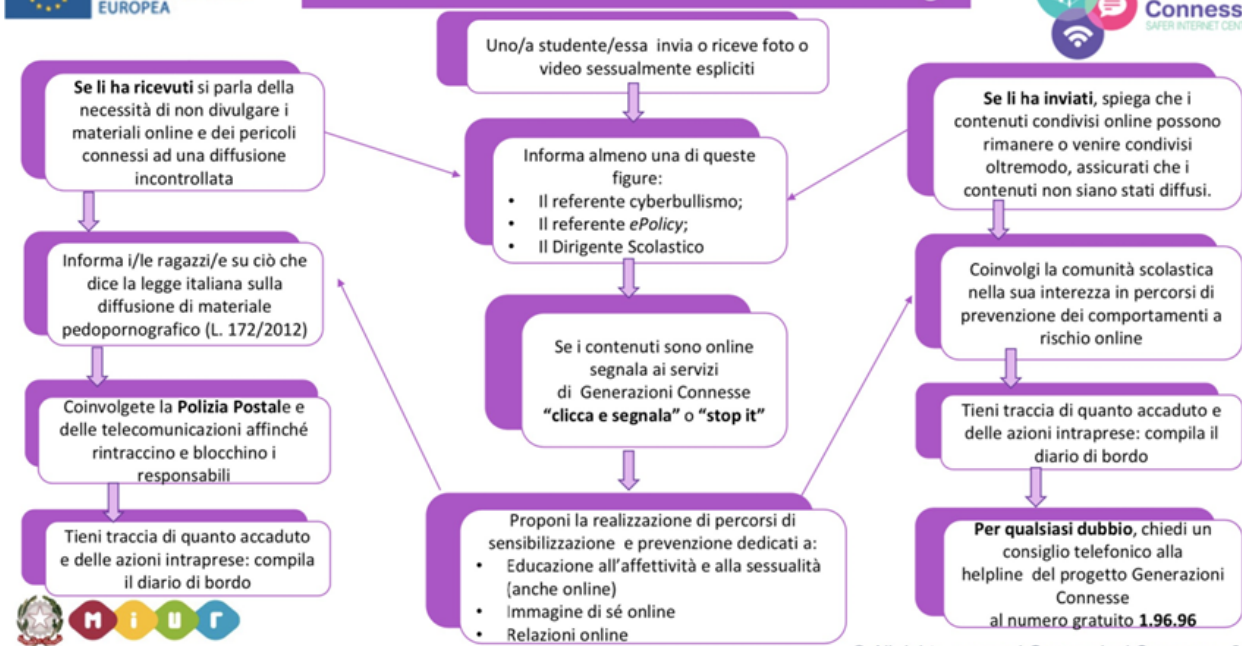


© All rights reserved Generazioni Connesse 2019

## Procedure interne: cosa fare in caso di sexting?

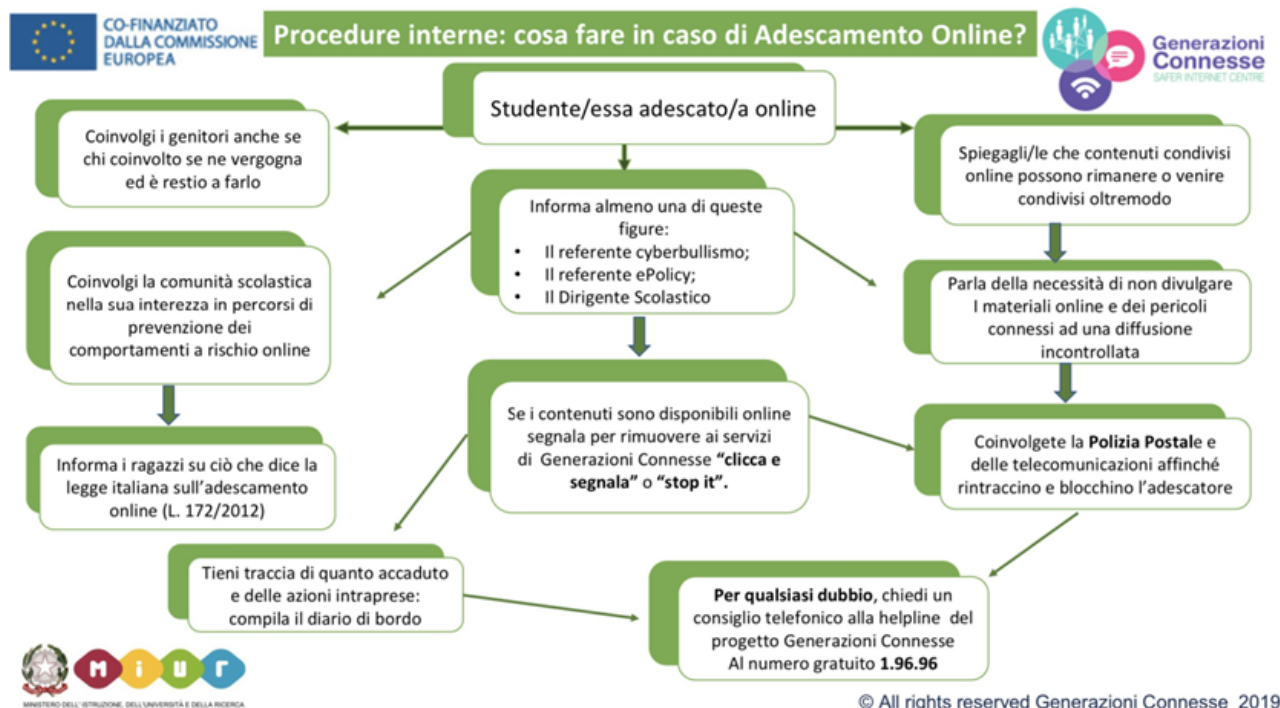


## Procedure interne: cosa fare in caso di Sexting?

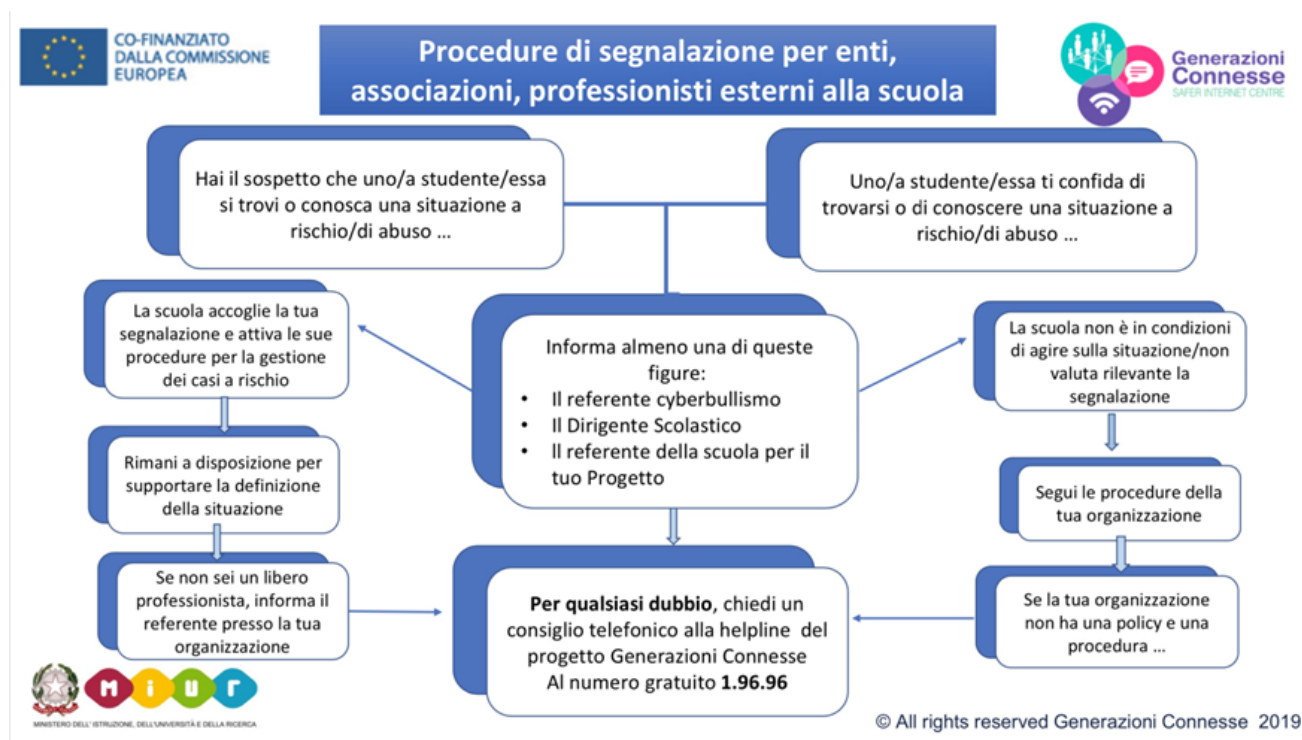


© All rights reserved Generazioni Connesse 2019

Procedure interne: cosa fare in caso di adescamento online?



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



*N.B. Le Schede di segnalazione di eventuali episodi di bullismo e cyberbullismo sono allegate al documento:  
**All.B\_Regolamento\_Bullismo\_Cyberbullismo\_DE FILIPPO DE RUGGIERO.***