ISTITUTO COMPRENSIVO DON ORIONE
Via Fabriano 4 - 20161 Milano C.M. MIIC8CS002 – C.F. 80130190152
TEL. 02 884452793 – FAX 02 88467996
e-mail: MIIC8CS002@ISTRUZIONE.IT sito: www.icsdonorione.edu.it
Plessi: scuola dell'infanzia di via Iseo 7 scuola primaria "F. Caracciolo" - via Iseo 7 scuola primaria "Don Orione" - via Fabriano 4
scuola secondaria di I grado "L. Da Vinci" - via Sand 32

Documento di ePolicy

ISTITUTO COMPRENSIVO STATALE
"DON ORIONE" – MILANO

Argomenti del Documento

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 alunni e delle alunne.

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 ePolicy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte degli alunni e delle alunne che degli adulti coinvolti nel processo educativo. L'ePolicy, 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'ePolicy 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.

1.2 - Ruoli e responsabilità

Affinché l'ePolicy 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

Il ruolo del Dirigente Scolastico è promuovere l'uso consentito delle tecnologie e di internet includendo i seguenti compiti:

• garantire la sicurezza on-line dei membri della comunità scolastica;

● garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti;

● garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);

● seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

Referenti di informatica di ciascun plesso

Il ruolo del referente di informatica include i seguenti compiti:

● stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;

● monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;

● assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione).

Direttore dei servizi generali e amministrativi

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 informatica della scuola sia funzionante, sicura e non aperta a uso improprio o a danno di 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 e delle alunne per la notifica di documenti e informazioni del Dirigente Scolastico nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca (educatori e personale ATA) include i seguenti compiti:

● informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;

● garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche e educative delle classi;

● garantire che gli alunni e le alunne capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;

● assicurare che gli alunni e le alunne abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;

● garantire che le comunicazioni digitali dei docenti con alunni e alunne e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;

● assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;

● controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni e delle alunne durante le attività scolastiche (ove consentito);

● nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni e le alunne a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;

● comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni e delle alunne (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;

● segnalare al Dirigente Scolastico qualsiasi abuso rilevato a scuola nei confronti degli alunni e delle alunne in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Alunni e alunne

Il ruolo degli alunni e delle alunne include i seguenti compiti:

● essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;

● avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;

● comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;

● adottare condotte rispettose degli altri anche quando si comunica in rete;

● esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

Il ruolo dei genitori degli alunni e delle alunne include i seguenti compiti:

● sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica;

● seguire gli alunni e le alunne nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;

● fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli e le figlie fanno di internet e del telefonino in generale.

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

Tutti gli attori che entrano in relazione educativa con gli alunni e le alunne 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 alunni e delle alunne 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 alunni e le alunne. 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'ePolicy all'intera comunità scolastica

Il documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli alunni e le alunne e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/alle alunni/e) si faccia a sua volta promotore del documento.

L'ePolicy viene condivisa e comunicata al personale, agli alunni e alle alunne, 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 alunni e le alunne 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 ePolicy

La scuola gestirà le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie,

valutando i diversi gradi di gravità di eventuali violazioni.

Disciplina degli alunni e delle alunne

Tra le potenziali infrazioni in cui è possibile che gli alunni e le alunne incorrano a scuola durante l'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, c'è **il collegamento a siti web non indicati dai docenti e un impiego dei dispositivi elettronici non autorizzato**. Gli interventi correttivi previsti per gli alunni e le alunne sono rapportati all'età e al livello di sviluppo dell'alunno e dell'alunna; infatti, più gli alunni e le alunne sono piccoli più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno e dell'alunna.

Sono previsti pertanto da parte dei docenti provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente Scolastico.

Per la scuola secondaria, si rimanda al Regolamento di Disciplina dell'Istituto.

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni e con le alunne, non connesso alle attività di insegnamento o al profilo professionale, anche tramite un'installazione di software o il salvataggio di materiali non idonei;
- un trattamento dei dati personali, comuni e sensibili degli alunni e delle alunne, 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 vigilanza elusa dagli alunni e dalle alunne che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti.

La valutazione di ciascun caso spetta al Dirigente Scolastico in collaborazione con tutto il personale, il quale potrà fornire ogni informazione utile per l'analisi. A seconda dell'infrazione commessa, si terrà conto delle procedure previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età degli alunni e delle alunne e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC. Le situazioni meno favorevoli sono:

- la convinzione che se il proprio figlio o la propria figlia rimangono a casa ad usare i dispositivi elettronici sono al sicuro e non combineranno guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio o propria figlia;
- una piena autonomia concessa al proprio figlio o alla propria figlia nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;

- un utilizzo dei dispositivi in comune con gli adulti che possono conservare in memoria materiali non idonei.

I genitori degli alunni e delle alunne possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge o soggetti a provvedimenti giudiziari, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato unitamente all'ePolicy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.
Nello specifico l'ePolicy richiede l'integrazione con l'inserimento delle seguenti norme:

Utilizzo del laboratorio di Informatica, delle postazioni di lavoro e dell'utilizzo di internet

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'Istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
4. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
5. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.
6. È vietato cancellare o alterare files-dati presenti sull'hard disk.
7. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione…).
8. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al Responsabile del laboratorio.
9. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà la segreteria personalmente o attraverso il Responsabile di laboratorio.
10. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su CD o pendrive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale.
3. È fatto divieto di usare software non conforme alle leggi sul copyright. È cura dell'insegnante utente di

verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio previa autorizzazione del Responsabile di laboratorio. Si raccomanda, quindi, di verificare che il software installato rispetti le leggi sul copyright.

4. È responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di CD/DVD per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.
2. Internet non può essere usato per scopi vietati dalla legislazione vigente.
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio internet.
4. È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'ePolicy 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.

Capitolo 2 - Formazione e curricolo

2.1 - Curricolo sulle competenze digitali per gli alunni e le alunne

Gli alunni e le alunne 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 alunni e le alunne verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale in riferimento al PTOF.

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

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli alunni e alle alunne modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

A tal fine e a seguito dell'emanazione della Legge 71/2017, il Dirigente Scolastico ha provveduto alla nomina di un Referente per il cyberbullismo (art.4 comma 3) e l'istituzione di un gruppo di lavoro aventi l'incarico di seguire il progetto MIUR "Generazioni Connesse". Nel triennio 2017/2019 è stato prodotto il primo documento di e-Safety Policy, quale indicatore del codice di condotta del nostro Istituto nella gestione della sicurezza informatica e nella prevenzione di atti di cyberbullismo. L'Istituto è attivamente rivolto verso proposte di miglioramento inerenti all'area informatica. La maggior parte del corpo docente dell'Istituto possiede conoscenze sulle TIC e le utilizza nella didattica. Ogni aula dei tre plessi dispone della LIM e frequente è l'impiego di questo strumento per proiezione video, presentazioni e impiego di software didattici.

La scuola si propone di supportare il corpo docente con corsi di formazione, affinché le conoscenze siano diffuse, collettive e oggetto di scambio tra i docenti stessi, attraverso momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo.

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 Scuola ha aderito ai seminari di formazione "Parole O_Stili" e provveduto a svolgere, in tutte le classi dell'Istituto, attività legate al "Manifesto della comunicazione non ostile e inclusiva"; tale documento sarà riportato sul diario dell'a.s. 2021/2022 prodotto dall'Istituto, come avviene ormai dall'a.s. 2017/2018. L'Istituto ha sempre collaborato inoltre con le forze dell'ordine per promuovere attività di sensibilizzazione/consapevolezza sull'utilizzo sicuro dei dispositivi.

2.4 - Sensibilizzazione delle famiglie e Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme 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.

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 alunni e sulle alunne 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.

3.2 - Accesso ad Internet

Accesso ad internet: filtri, antivirus e sulla navigazione

Data la giovane età degli alunni e delle alunne del nostro Istituto, è fondamentale fare tutto il possibile per evitare l'esposizione a contenuti inappropriati.

Gli alunni e le alunne non sono mai lasciati soli nelle aule in cui sono presenti dei computer collegati ad internet.

I computer portatili collocati nelle aule accedono ad internet attraverso rete WIFI, nel laboratorio informatico sono presenti computer fissi che accedono tramite rete LAN.

Le scuole dell'Istituto sono dotate di antivirus, monitorati e tenuti aggiornati dai Responsabili dei laboratori informatici.

Gestione accessi

L'accesso a internet è possibile e consentito per la didattica in tutte le aule e nei laboratori multimediali. Solo il docente dalla propria postazione può consentire agli alunni e alle alunne di accedere a internet. Le postazioni non sono dotate di webcam. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list e consentono il collegamento solo a siti idonei alla didattica. Tutte le aule sono dotate di pc, portatili o fissi, per lo svolgimento di lezioni multimediali sia per la compilazione del registro elettronico. Tutti i computer della scuola hanno un accesso con password per gli strumenti di amministrazione, hanno invece un accesso libero per l'utente generico.

La connessione alla rete wi-fi è riservata ai docenti, che possono utilizzare anche dispositivi personali, per fini didattici. Per tutto il personale della scuola la connessione alla rete wi-fi è accessibile tramite una password unica.

Le postazioni presenti in segreteria sono accessibili solo dal personale amministrativo con utenza e password dedicate.

E-mail

Per l'invio di circolari e comunicazioni da parte del Dirigente, sono state create mailing list per tutti i docenti dell'Istituto, suddivise per ordine di scuola e per plessi.

La segreteria ha un proprio account di posta elettronica utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

Sito web della scuola

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo http://www.icsdonorione.edu.it Il Dirigente Scolastico e lo staff verificano i contenuti destinati alla pubblicazione e ne valutano la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.…

Social network

Attualmente l'istituzione scolastica non ha creato una pagina social col proprio profilo o ha autorizzato il personale scolastico a utilizzarli per nome e per conto della stessa. La scuola, però, fa talvolta ricorso a Youtube come fonte per reperire materiale video didattico online. A partire dal 2020, inoltre, l'istituzione scolastica fa uso della piattaforma Weschool, utilizzata inizialmente per la didattica a distanza, ora anche come mezzo per la condivisione di materiali, di attività e di comunicazione con gli alunni e le alunne ai fini della didattica digitale integrata. Il suo utilizzo è disciplinato dal Piano e dal Regolamento per la DDI caricati sul sito della 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. A tal fine, la scuola si è dotata di un registro elettronico: RE Axios, un software che permette di interagire in tempo reale con tutti i dati che la scuola vuole rendere disponibili ai destinatari (segreteria, docenti, famiglia). La sicurezza e la privacy, nonché le prerogative di accesso, sono controllati mediante chiavi d'accesso individuali, generate da un'apposita procedura interna e comunicati ai destinatari a mezzo posta elettronica o cartacea. La consultazione del registro permette di osservare le assenze/ritardi/permessi e giustificazioni per mese, per giorno e per materia. Permette inoltre di verificare i compiti assegnati nel registro di classe da parte del docente, l'indicazione degli argomenti trattati, eventuali comunicazioni da parte del Dirigente Scolastico o dei docenti e l'andamento dell'alunno o dell'alunna.

3.4 - Strumentazione personale

La tecnologia fornisce agli alunni e alle alunne opportunità innovative e inedite per incrementare la loro cultura. La scuola intende favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento. In riferimento al Decalogo per l'uso dei dispositivi mobili a scuola (BYOD – Bring Your Own Devices) inserito nel Piano Nazionale Scuola Digitale per la Secondaria di Primo Grado si prevede quanto segue:

1. Sono ammessi in classe i seguenti dispositivi digitali mobili: cellulare, tablet, e-reader, pc soltanto per attività didattiche programmate, di cui saranno informate le famiglie e su esplicita richiesta da parte del docente.
2. È vietato collegarsi, scaricare/caricare/copiare materiale da Internet, inviare e-mail senza il permesso del docente.
3. È vietato agli alunni e alle alunne usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto in classe senza il permesso dell'insegnante. La scuola predispone un modello di liberatoria sull'utilizzo di materiale audio video per fini didattici.
4. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione intestati ufficialmente all'Istituto da cui potranno essere condivisi.
5. Gli alunni e le alunne sono responsabili personalmente dei propri dispositivi.
6. L'Istituzione Scolastica non sarà ritenuta responsabile in alcun modo dei dispositivi personali degli alunni e delle alunne.
7. L'uso inappropriato dei dispositivi digitali mobili all'interno dell'ambiente scolastico e durante le uscite didattiche e i viaggi di istruzione verrà sanzionato in misura della gravità come stabilito dal Regolamento di Disciplina; poiché i moderni cellulari possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle ad altri utenti, si ricorda che eventi di questo tipo – se si concretizzano durante l'orario scolastico – si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.
8. L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli alunni e le alunne dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o sparizioni di telefonini cellulari, di lettori mp3, di hard/disk portatili o pendrive.

Capitolo 4 - Rischi on line: prevenzione, rilevazione e gestione dei casi

4.1 - Sensibilizzazione

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 gli alunni e le alunne 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.

4.2 - Prevenzione

Rischi

1. Quando si inizia a navigare con i Social Network e le applicazioni web, bisogna informarsi sui diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.
2. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato, perché il materiale pubblicato può rimanere disponibile online anche per molto tempo e il suo uso può diventare incontrollabile.
3. È indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse.
4. Se si condividono elementi multimediali o informazioni che riguardano altre persone, è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare video girati di nascosto o dove sono presenti persone filmate senza il loro consenso.
5. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti adeguati, indicando abuso, data, ora, utenti e servizio coinvolti.

Azioni

La scuola si impegna a:

1. riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la Legge sulla privacy (art. 41 f del D.Lgs. 196/2003).

I docenti si impegnano a:

1. accompagnare gli alunni e le alunne nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi;
2. approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyberbullismo;
3. garantire la presenza di una commissione che promuova attività informative e formative sul fenomeno del bullismo e del cyberbullismo;
4. confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;
5. informare il referente per il bullismo e cyberbullismo su casi rilevanti.

I genitori si impegnano a:

1. prendere visione del Regolamento d'Istituto;
2. firmare il Patto di Corresponsabilità redatto dall'Istituto;
3. prendere visione della E-Safety Policy messa a disposizione sul sito dell'Istituto http://www.icsdonorione.edu.it;
4. seguire le azioni promosse dalla scuola per un uso corretto della Rete.

Gli alunni e le alunne si impegnano a:

1. prendere visione del Regolamento d'Istituto;
2. prendere visione e firmare il Patto di Corresponsabilità;
3. prendere visione della E-Safety Policy messa a disposizione sul sito dell'Istituto http://www.icsdonorione.edu.it;
4. rispettare le regole per un uso corretto della tecnologia;
5. segnalare casi di abuso online alla famiglia o a adulti di riferimento, fra cui gli insegnanti.

4.3 - Rilevazione

Che cosa segnalare

1. Contenuti afferenti alla privacy e non autorizzati (foto o video personali, l'indirizzo di casa o il telefono, informazioni private proprie o di altri, ecc.);
2. Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto e video imbarazzanti, virus, contenuti razzisti o inneggianti al suicidio, immagini o video umilianti, insulti, ecc.);
3. Contenuti afferenti alla sessualità (messaggi molesti, conversazioni che connotano una relazione intima, foto e video personali con nudità o abbigliamento succinto, immagine pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali, ecc.).

Come segnalare: quali strumenti e a chi

Per il telefono cellulare, ci si può assicurare che l'alunno o l'alunna vittima salvi sul suo telefono ogni messaggio, testo o immagine, conservando così il numero del mittente.

Qualora ci si dovesse accorgere che l'alunno o l'alunna stia usando uno strumento in modo inappropriato (cellulare, tablet, pc), l'insegnante deve conservare copia dei contenuti di tale azione.

Come gestire le segnalazioni

Per il telefono cellulare e in presenza di contenuti evidenti, si può informare la famiglia e richiedere la consegna temporanea dello strumento quale prova per la segnalazione. Qualora non si disponga di prove, le notizie raccolte devono comunque essere comunicate ai genitori e, per fatti rilevanti, anche al Dirigente Scolastico. In particolare, la segnalazione viene fatta ad entrambe le famiglie (vittime e autore della condotta negativa).

Per la segnalazione di fatti rilevati, sono previsti i seguenti strumenti:

- segnalazione al Consiglio di Classe, valutando le singole situazioni, e comunicazione scritta ai genitori;
- relazione scritta al Dirigente Scolastico (per casi rilevanti);
- convocazione scritta e colloquio con i genitori degli alunni o delle alunne coinvolti.

Per i reati più gravi, gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria o agli organi di polizia competenti.

4.4 - Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso

Gestione dei casi di "immaturità"

Le interazioni animate, i contrasti verbali o la presa in giro "per gioco" vengono controllati e contenuti dai docenti attraverso i normali interventi educativi di richiamo al rispetto delle regole di convivenza civile, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gestione dei casi di "prepotenza" o "prevaricazione"

I comportamenti definibili "bullismo" sono caratterizzati da atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, emarginazione a danni di una o più persone in un rapporto asimmetrico (disuguaglianza di forze di potere) e con disagio delle vittime. Nel caso del Cyberbullismo le molestie sono attuate attraverso strumenti tecnologici., con invio di messaggi in chat, sms e e-mail offensive o di minaccia, foto compromettenti o denigratorie pubblicate in rete.

Gli interventi devono essere mirati sul gruppo classe e gestiti in collaborazione dai docenti della classe e d'intesa con le famiglie. Inoltre, è opportuno intraprendere percorsi individualizzati di sostegno alle vittime, volti ad incrementare l'autostima e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una condivisione delle norme morali. Infine, la scuola, qualora rilevi una situazione psico-socioeducativa particolarmente problematica, convoca i genitori per valutare con loro a quali risorse territoriali possono rivolgersi.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Gestione degli "abusi sessuali"

In generale si parla di abuso sessuale sui bambini quando un bambino viene coinvolto in un atto sessuale. Ciò è caratterizzato dal fatto che il bambino non comprende del tutto tale atto, non è informato e quindi non è in grado di acconsentire, oppure sulla base del suo livello di sviluppo non è ancora pronto per tale atto e non può dare il proprio consenso.

Per questi casi è prioritaria la segnalazione al Dirigente Scolastico e la conseguente denuncia all'autorità giudiziaria o agli organi della Polizia, passo indispensabile per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

Il compito della scuola non è comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali e educativi che possono aiutare il bambino a riprendere una crescita serena.

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.

Capitolo 5 - Segnalazione e gestione dei casi

5.1 - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli alunni e dalle alunne, 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 alunni e le alunne 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 alunni e le alunne 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.

5.2 - Strumenti a disposizione di alunni e alunne

Per aiutare alunni e alunne 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;
- docente referente per le segnalazioni, docenti di classe o qualsiasi adulto di riferimento.

Anche gli alunni e le alunne, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 oppure possono fare segnalazione, anche in forma anonima, utilizzando Youpol, app ufficiale della Polizia di Stato.

5.3 - Gli attori sul territorio

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

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse

"Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

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

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

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

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

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

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

Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

All'interno della sezione dedicata al progetto "Generazioni Connesse" e alla ePolicy si possono trovare i seguenti allegati con le procedure da seguire nel caso di situazioni di rischio:

- Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?
- Procedure interne: cosa fare in caso di evidenza 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
- Volantino informativo della Polizia di Stato sull'app Youpol
- Scheda di segnalazione di Generazioni Connesse
- Scheda di segnalazione al Garante per la protezione dei dati personali