Liceo Statale
Enrico Fermi
Cecina

Documento di E-policy

INTRODUZIONE

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. Le "competenze digitali" sono fra le abilità chiave all'interno del quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente). In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. PRESENTAZIONE DELL'EPOLICY

1.1 Scopo della 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.

Scopo del presente documento è quello di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. In particolare, essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzare all'adozione di buone pratiche, quando sono fuori dalla scuola. Il Liceo Fermi di Cecina, come tutte le scuole italiane del XXI secolo, accoglie i "nativi digitali" che, anche in prossimità della maggiore età, sono esposti a rischi di cui sono inconsapevoli. Pertanto, la nostra scuola ha deciso di dotarsi di misure di prevenzione, controllo e formazione di allieve, allievi e famiglie, allo scopo di ridurre al minimo la frequenza di atti che non solo creano disagio nella comunità scolastica, ma possono anche configurarsi come "reati".

Infatti, se gli adolescenti mostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, è anche vero che, assai frequentemente, a questa abilità non corrisponde un'adeguata e corretta capacità interpretativa della mole di informazioni, alle quali essi sono di continuo sottoposti, in primo luogo attraverso i social network, che, se utilizzati in modo superficiale e inappropriato, possono trasformarsi in veicoli di reati e comportamenti scorretti verso gli altri. Questo documento nasce, dunque, dall'esistenza di questo bisogno di promozione di un uso sicuro e positivo delle tecnologie, per cui è in atto anche la scrittura, da parte di alcuni studenti, di una *netiquette:* si tratta di due regolamenti prodotti dalla Scuola nell'ambito del progetto "Generazioni connesse", promosso dal Miur. La sua intenzione è di offrire alle Istituzioni Scolastiche interessate, un supporto effettivo nella definizione di misure di prevenzione, rilevazione e gestione delle problematiche derivanti da un uso non consapevole delle tecnologie digitali tra gli studenti (anche attraverso la formazione degli insegnanti e la sensibilizzazione dei genitori).

In sintesi, il documento intende semplicemente costituire un primo passo in questa direzione e fornire alcune linee guida rispetto alle azioni dell'Istituto in ordine a:
1) utilizzo consapevole delle TIC in ambiente scolastico e nella didattica
2) prevenzione e gestione di situazioni problematiche connesse all'uso delle tecnologie digitali.

Gli utenti, siano essi docenti o alunni, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare, per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

1.2.1 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, si impegni nella sua attuazione e promozione.

La comunità degli adulti ha un ruolo fondamentale nel garantire che gli adolescenti utilizzino le nuove tecnologie in modo adeguato e sicuro. Si tratta di un impegno che coinvolge chiunque rivesta un ruolo educativo e non soltanto gli insegnanti, ma anche i genitori e l'intera comunità scolastica. Va da sé che in un percorso di graduale acquisizione della capacità di gestire in positivo le proprie competenze digitali, gli studenti abbiano un ruolo di primo piano. Essi potranno, dunque, essere coinvolti non solo in quanto destinatari, ma anche come interlocutori attivi di azioni e interventi finalizzati alla piena attuazione della Policy. La stesura da parte di alcuni di loro di una *netiquette d'Istituto* rappresenta proprio questa co-partecipazione della compagine studentesca.

Al **Dirigente Scolastico** compete l'approvazione del presente documento e di ogni sua eventuale revisione, nonché la valutazione dell'efficacia, il monitoraggio, l'attività di indirizzo nell'attuazione della E-Policy. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'**Animatore Digitale** e il **Team per l'Innovazione Digitale** collaborano alla redazione e alle eventuali revisioni della E-Policy, inoltre, come da Piano Nazionale Scuola Digitale (PNSD), agiscono nell'ambito di strumenti e infrastrutture, contenuti

e competenze, formazione e accompagnamento e dunque provvedono a stimolare la formazione interna alla Scuola in tali ambiti. Essi promuovono percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica).

I **Docenti** hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Essi possono integrare, infatti, parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso delle tecnologie della Rete; contribuiscono allo sviluppo delle competenze digitali, della conoscenza e del rispetto delle norme di sicurezza per un corretto utilizzo del web e delle tecnologie digitali, sia in ambiente scolastico, sia nelle attività extrascolastiche; segnalano alle famiglie eventuali problemi emersi nell'attività scolastica in merito all'uso del digitale; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il **Personale ATA**, consapevole delle questioni di sicurezza informatica, segnala ai Docenti, al Dirigente Scolastico o ai suoi collaboratori eventuali abusi da parte degli alunni.

Gli **Studenti** sono responsabili di un corretto utilizzo dei dispositivi informatici e delle tecnologie digitali. Essi sono tenuti a:

- non utilizzare dispositivi personali durante l'attività didattica, quando non dichiaratamente consentito dai docenti;
- conoscere l'importanza dell'adozione di buone pratiche di sicurezza informatica in ogni momento della vita, allo scopo di tutelare sé stessi e gli altri;
- comprendere l'importanza di segnalare eventuali abusi ed usi impropri;
- essere consapevoli del significato e della gravità del fenomeni di cyber-bullismo e tutti gli altri fenomeni che si connotano come reati secondo l'ordinamento giuridico italiano.

Genitori e familiari svolgono un ruolo fondamentale nel guidare gli alunni verso una crescente consapevolezza nel corretto utilizzo di Internet e dei dispositivi mobili. La scuola continuerà a sensibilizzare e informare le famiglie in questo senso, attraverso incontri ed eventi, aperti anche ad essi. L'auspicio è che, se coinvolti come parte attiva, i genitori, specialmente quelli degli alunni del biennio, siano motivati a sostenere la Scuola nel promuovere, presso i loro figli, buone pratiche e un uso appropriato di immagini digitali e video, registrati anche in ambiente extrascolastico.

1.2.2 Comportamento di studenti, docenti e tecnici durante l'attività didattica

Il docente nel libero esercizio della sua professionalità può avvalersi dei seguenti strumenti: postazioni PC, tablet, smartphone, LIM nelle classi e nei laboratori e deve:

- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento;
- controllare l'uso da parte degli alunni delle tecnologie digitali durante l'attività didattica;
- dare chiare indicazioni sul corretto utilizzo della rete (internet, piattaforme studenti, app educative, ecc.);
- assumersi la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti ai tecnici di laboratorio;
- non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;
- non eseguire tentativi di modifica della configurazione di sistema delle macchine, non istallare e non scaricare programmi autonomamente dal web;
- non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili, propri o degli alunni.

Gli studenti sono tenuti a:

- utilizzare le TIC su indicazioni del docente;
- accedere all'ambiente di lavoro con il corretto account;
- accedere esclusivamente ai contenuti e alle pagine web indicate dal docente;
- archiviare i propri documenti in maniera ordinata e all'interno della cartelle del disco condiviso predisposte dal tecnico di laboratorio;
- in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
- non eseguire tentativi di modifica della configurazione di sistema delle macchine, non istallare e non scaricare programmi autonomamente dal web;
- non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
- chiudere correttamente la propria sessione di lavoro.

I tecnici informatici sono tenuti ad:

- accedere e controllare tutti i files, i programmi e lo status dei dispositivi del laboratorio d'informatica;
- monitorare il buon funzionamento e la sicurezza delle TIC e dei dispositivi del laboratorio;
- limitare attraverso un proxy l'accesso ad alcuni siti;
- curare la prenotazione dei laboratori affinché sia tenuta traccia di ora e laboratorio utilizzati da ciascuno.
- Essi sono gli unici autorizzati ad installare nuovi software;
- sono inibiti dalla presenza in aula durante le attività didattiche, per motivi di privacy, a meno che la loro presenza non sia necessaria per motivi di sicurezza o su richiesta del docente in servizio.

1.2.3 Informativa per i soggetti esterni che erogano attività educative nell' Istituto

Al fine di rendere l'E-Policy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, il Liceo Fermi di Cecina consegnerà una sintesi della stessa alle organizzazioni/associazioni extrascolastiche e agli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo. Un'informativa sintetica sull'E-Policy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali. Tale documento sintetico sarà redatto dopo l'approvazione della seguente E-policy da parte del Consiglio d'Istituto e dovrà chiarire il sistema di azioni e le procedure di segnalazione da seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1.3 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/alle studenti/esse) si faccia a sua volta promotore del documento. 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.

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;
- Attività didattiche ad hoc promosse nelle prime settimane di lezione.

1.4 Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. Sarà opportuno mettere in atto, preventivamente, attività laboratoriali miranti a sviluppare negli alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente ed improprio del web e che forniscano loro, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

I provvedimenti disciplinari nei confronti dello studente che abbia commesso un'infrazione alla policy a seguito di un comportamento scorretto, messo in atto durante l'orario scolastico o comunque attinente alla vita scolastica (ad esempio cyberbullismo sulla chat del gruppo classe), dovranno essere proporzionati all'età dello studente, al contesto dell'infrazione compiuta e alla gravità dell'infrazione commessa e potranno essere così graduati:

- richiamo verbale;
- sanzioni commisurate alla gravità della violazione commessa (dalla assegnazione di attività da svolgere a casa su temi di Cittadinanza e Costituzione fino alla sospensione);
- divieto temporaneo di prendere parte ad alcune iniziative scolastiche;
- provvedimento disciplinare sul registro elettronico al fine di informare ai genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

Qualora tali infrazioni dovessero configurarsi come reato, ne sarà data tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del Codice di Procedura Penale). Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la

posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Per 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, saranno attivate le procedure previste dalla legge e dai contratti di lavoro.

1.5 Monitoraggio dell'implementazione della e-Policy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola, sulla base anche dei casi problematici riscontrati e della loro gestione.
Il monitoraggio dell'implementazione della policy e il suo eventuale aggiornamento sarà svolto dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale, del DPO, dall'amministratore di sistema e dal Referente Bullismo e Cyber bullismo.

1.6 Integrazione dell'e-Policy con Regolamenti esistenti

La E-policy è coerente con ciò che è previsto e stabilito dai Regolamenti di Istituto esistenti, in particolar modo con i regolamenti di utilizzo dei laboratori informatici, oltre ad essere in linea con quanto espresso dal Patto di Corresponsabilità, dalle linee guida MIUR e dalle indicazioni generali sui temi in oggetto. Il documento si integra con le linee del PTOF, con il regolamento di istituto e la Netiquette contenuta nell'informativa all'utilizzo dell'account GSuite di istituto.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più intuitivo ed agile rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale, in costante aggiornamento. All'interno del PNSD il Liceo Fermi porta avanti azioni volte all'utilizzo della didattica inclusiva e digitale, attraverso le piattaforme Moodle, G suite e le classi virtuali.

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

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC (Tecnologie dell'Informazione e della Comunicazione) 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. In caso di chiusure forzate della scuola, la scuola offre forme di didattica a distanza, così come è successo durante la preoccupante situazione di diffusione del "coronavirus", quando i Ministeri della Salute e della Scuola, in modo unitario, hanno suggerito di evitare le lezioni in presenza. La nostra scuola si attiva ogni anno per rendere possibile lo svolgimento di attività di (auto) aggiornamento, che includono i metodi di insegnamento a distanza, la conoscenza di programmi o software adeguati allo scopo, la sicurezza on line e i temi della privacy e cyber bullismo.

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

Il Liceo Fermi di Cecina 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, team dell'innovazione) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio, delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti. L'obiettivo sarà quello di una formazione continua sull'utilizzo e l'integrazione delle TIC nella didattica ma anche sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali.

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 gli adolescenti 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, 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'impegno del Liceo Fermi nei prossimi anni sarà anche quello di predisporre incontri formativi per i genitori degli studenti in ingresso, o comunque frequentanti il biennio, sui temi della sicurezza in rete e dell'educazione della cittadinanza digitale.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT

3.1 Protezione dei dati personali

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

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni. La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati). Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

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

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

Fra questi, particolarmente importanti sono:

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

Per trattamento dei dati s'intende qualsiasi operazione, compiuta con o senza l'ausilio di processi automatizzati, applicata a dati personali o insiemi di dati personali. Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679). I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Il nostro Liceo in conformità al al Regolamento UE 2016/679 deve:

- ✦ Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.
- ✦ Valutare i rischi sulla privacy relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli alunni, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli alunni, come i dati vaccinali con le Asl.
- ✦ Analizzare il processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara

(art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

- ✦ Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:
  - ◦ analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati
  - ◦ proposte in messa in sicurezza della intranet scolastica
  - ◦ sulle reti Wi-fi installate;
  - ◦ utilizzo di black-list per la navigazione (sistemi di filtraggio dei contenuti);
  - ◦ uso di un firewall hardware (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole);
  - ◦ istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub-incaricati del trattamento.

3.2 Accesso ad internet

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola". Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

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

- L'accesso a internet è possibile e consentito per la didattica in tutti i plessi del biennio e triennio attraverso reti WiFi e cablate; al momento l'accesso per I dispositivi personali degli studenti non è previsto, quindi le credenziali delle WiFi non devono essere loro fornite, e il lavoro sulle postazioni fisse è vigilato e mediato dai docenti. Singoli studenti possono essere autorizzati mediante il controllo centralizzato delle reti.
- Le reti interne accessibili a studenti e docenti sono protette tramite filtraggio dei contenuti e/o gestione centralizzata della sicurezza tramite Firewall e Server DNS specifici.
- Le condivisioni di file locali dei laboratori sono gestite e sorvegliate dal personale docente e tecnico.
- Nessun utente ha privilegi amministrativi sulle postazioni di lavoro. Essi sono riservati agli amministratori di sistema.
- Tutte le postazioni sono munite di antivirus o misure di protezione equivalenti.
- Le postazioni amministrative sono sottoposte a backup automatizzati. Un server NAS sottoposto a regolare scansione antivirus e aggiornamento di sistema contiene la maggioranza dei dati di backup.
- Le postazioni non amministrative sono munite di sistemi automatici per la cancellazione dei dati privati dai browser Mozilla Firefox e Google Chrome al momento dell'avvio.
- La grande maggioranza delle postazioni utilizza come sistema operativo una distribuzione GNU/Linux configurata per un'elevata sicurezza. Gli aggiornamenti sono automatici e trasparenti per l'utente.
- L'accesso alla rete è comune per ogni plesso e permette tramite rete LAN o Wifi (talvolta attraverso l'impostazione di una password) di accedere al web per esigenze didattiche e per redigere giornalmente il registro elettronico.

3.3 Strumenti di comunicazione online e registro elettronico

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:
Il personale docente, ATA e gli studenti i cui consigli di classe hanno aderito al progetto Classroom hanno un account mail di istituto. Per gli studenti, l'account viene rilasciato dietro autorizzazione dei genitori, previamente informati con apposita documentazione e autorizzazione. Ogni ufficio è dotato di un account di posta elettronica che sarà utilizzato ordinariamente dagli uffici per l'invio della documentazione di servizio. La posta elettronica istituzionale gestita dalla segreteria

è protetta da antivirus, e quella certificata anche dall'antispam. Tutte le postazioni sia amministrative che pubbliche sono configurate in modo da non essere suscettibili ai virus trasmessi tramite la posta elettronica. A ciò si aggiungono i meccanismi di protezione dovuti alla gestione web centralizzata della posta elettronica istituzionale e certificata. Gli indirizzi di posta elettronica gestiti tramite la Google Suite impiegano i meccanismi di protezione forniti dal produttore. Il registro elettronico è uno strumento per docenti, famiglie e studenti, che consente l'aggiornamento in tempo reale sul progresso scolastico, in termini di voti e argomenti svolti, e sulle presenze in aula. All'atto dell'iscrizione, alle famiglie vengono fornite le credenziali per accedere alle app collegate. Per ció che concerne il sito web della scuola, la dirigenza attualmente vi pubblica i contenuti delle proposte formative e del settore didattico, nonché le circolari ed avvisi. Costantemente i docenti sperimentano l'uso di piattaforme didattiche protette: *social learning* interamente dedicati alla didattica per creare classi virtuali, condividere risorse, realizzare contenuti multimediali, assegnare verifiche e dialogare in maniera "social" tra docenti, studenti e famiglie.

3.4 Strumentazione personale BYOD

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli studenti 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.

4. RISCHI ON LINE: CONOSCERE, PREVENIRE E RILEVARE

4.1 Sensibilizzazione e prevenzione dei rischi on-line

Si possono verificare due situazioni di rischi:

1. uso improprio degli strumenti personali, per scopi non didattici, anche in spazi diversi dall'aula; acquisire e pubblicare in rete foto o video propri o di altri, anche a contenuto improprio; pubblicare messaggi o commenti lesivi della dignità o della reputazione altrui; accedere a contenuti e siti non adatti ai minori; ascoltare musica; utilizzare giochi, chat, ecc.; entrare in contatto con sconosciuti.
2. navigazione in internet mediante gli strumenti presenti a scuola; accedere a contenuti inappropriati; infettare i computer o i tablet con virus o malware scaricando materiali, o installando programmi e applicazioni o utilizzando dispositivi personali di memoria; utilizzare materiale illegale; violare il diritto d'autore o di proprietà.

Il rischio online si configura come la possibilità per lo studente di:

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

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. È importante che gli adolescenti 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 ragazze e ragazzi, tra cui anche l'implementazione e il miglioramento della navigazione in internet tramite:

- installazione di filtri sul server e sul motore di Ricerca
- il blocco di finestre pop up,
- verifica della cronologia
- utilizzo di cloud

Il Liceo Fermi s'impegna ad organizzare, ogni anno, uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli studenti, con il coinvolgimento di esperti. Il Liceo Fermi, s'impegna altresì a pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola, nonché a promuovere, ogni anno e in ogni classe, attività di studio e dibattito a partire dalla *netiquette d'istituto* compilata dagli alunni stessi.

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. Seguendo le citate linee guida, il Liceo Fermi s'impegna a:

- individuare e formare un referente d'Istituto;
- sviluppare le competenze digitali tra gli studenti all'interno degli obiettivi formativi prioritari (L.107/2015);
- promuovere di ruolo attivo degli studenti in attività di peer education;
- prevedere misure di sostegno e rieducazione dei minori coinvolti;
- prevedere azioni preventive ed educative e non solo sanzionatorie.

Il Referente d'Istituto per le iniziative di prevenzione e contrasto di bullismo e cyberbullismo ha il compito di coordinare, assieme all'Animatore Digitale, le iniziative di prevenzione e contrasto. Per la prevenzione si fa riferimento a quando disposto nel paragrafo 4.1. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

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. Per la prevenzione si fa riferimento a quando disposto nel paragrafo 4.1.

4.4 Dipendenza e Gambling: che cos'è e come prevenirlo

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. Per la prevenzione si fa riferimento a quando disposto per bullismo e cyberbullismo.

4.5 Sexting: che cos'è e come prevenirlo

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. Per la prevenzione si fa riferimento a quando disposto nel paragrafo 4.1.

4.6 Adescamento online: che cos'è e come prevenirlo

l *grooming* (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre gli 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 – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012). Per la prevenzione si fa riferimento a quando disposto nel paragrafo 4.1.

4.7 Pedopornografia: che cos'è e come prevenirlo

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. 38 del 6 febbraio 2006 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. La pedopornografia, pur essendo un tema molto delicato, 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. Per la prevenzione si fa riferimento a quando disposto nel paragrafo 4.1.

5.1 Gestione dei casi: Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno studente possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite. 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 (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti e studentesse in difficoltà.

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono: si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. Gli insegnanti sono chiamati a essere *torre di avvistamento*, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno.

- **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?). È necessario poi valutare l'eventuale stato di disagio vissuto dagli studenti coinvolti (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi all'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.

- **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, e il blocco della sua diffusione via dispositivi mobili.

5.2 Gestione dei casi: Come segnalare

Per aiutare studenti e studentesse 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;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è sempre opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire. I docenti sono chiamati a predisporre delle rilevazioni e qualora si rendano conto che si trovano di fronte a situazioni di criticità dovranno compilare il modulo secondo protocollo che sarà trasmesso alla Dirigenza Scolastica. I docenti difatti avranno a disposizione uno strumento di rilevamento delle criticità, sul quale descrivere le situazioni che si vengono a determinare, indicando anche le azioni messe in atto (vedi allegato).

La scuola non può intervenire su ciò che gli alunni svolgono fuori da essa con strumenti digitali, ma qualora il docente venisse a conoscenza di eventuali atti scorretti, come la condivisione di foto non autorizzate o l'insulto da parte di un alunno ad un compagno sul gruppo classe di WhatsApp (la creazione dei gruppi classe su WhatsApp è oggi una pratica molto diffusa) o su altro social network, tempestivamente dovrà invitare le famiglie degli alunni coinvolti ad un attento monitoraggio delle attività svolte dai propri figli in rete e, nei casi più gravi, seguire la procedura indicata nella tabella con la compilazione del modello di rilevazione. La segnalazione dei casi di bullismo e cyberbullismo dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (allegato 1) che avrà il compito di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

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. Esistono, inoltre, i seguenti servizi: - Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze; - STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Gli episodi di bullismo avvenuti in ambito scolastico e che siano stati accertati devono essere subito sanzionati, privilegiando il ricorso a sanzioni disciplinari di tipo riparativo, convertibili in attività a favore della comunità scolastica, anche in conformità con quanto indicato nella direttiva del Ministero della Pubblica Istruzione

n. 16 del 5 febbraio 2007 e nello Statuto delle studentesse e degli studenti della scuola secondaria D.P.R. 21 novembre 2007 n.235 “Regolamento recante modifiche ed integrazioni al D.P.R. 24 giugno 1998 n. 249” (Testo in vigore dal 2 gennaio 2008). Le competenze in materia disciplinare, se il comportamento trasgressivo è previsto dal regolamento disciplinare d’Istituto, redatto in conformità alle norme sopraindicate, spettano al Consiglio di classe. Le sanzione disciplinari irrogate dalla scuola non sostituiscono né sono sostituite da eventuali sanzioni penali se il comportamento violento e prevaricatore si configura come reato, né quelle civili per eventuali danni ingiustamente causati a cose o a persone.

Liceo Statale
Enrico Fermi
Cecina

MODULO PER LA SEGNALAZIONE DI EPISODI DI BULLISMO E/O CYBERBULLISMO

SEXTING, REVERNGE-PORN, HATE SPEECH

(Descrizione guidata dell'episodio a cura dell'insegnante o del professionista esperto)

NOME E COGNOME DELLO STUDENTE:

_____

CLASSE: _____ PLESSO: _____

Che cosa è successo?

_____

_____

_____

_____

_____

_____

_____

Quando? Gli episodi si ripetono?

_____

Ricaduta sui social?

_____

_____

_____

_____

Chi è stato?

_____

Chi è ne testimone?

_____

_____

Quali altri insegnanti ne sono a conoscenza?

_____

I tuoi genitori ne sono a conoscenza?

_____

Azioni intraprese e concordate con il DS:

_____

_____

_____

_____

_____

_____

Data _____

Docente _____

Dirigente _____

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Generazioni Connesse SAFER INTERNET CENTRE

Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori).
Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.

Valuta se è il caso di avvisare il consiglio di classe.
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggerisci di **chiedere aiuto** per situazioni di questo tipo.
Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Se emergono evidenze passa allo schema successivo

Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017)
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

Generazioni Connesse SAFER INTERNET CENTRE

Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

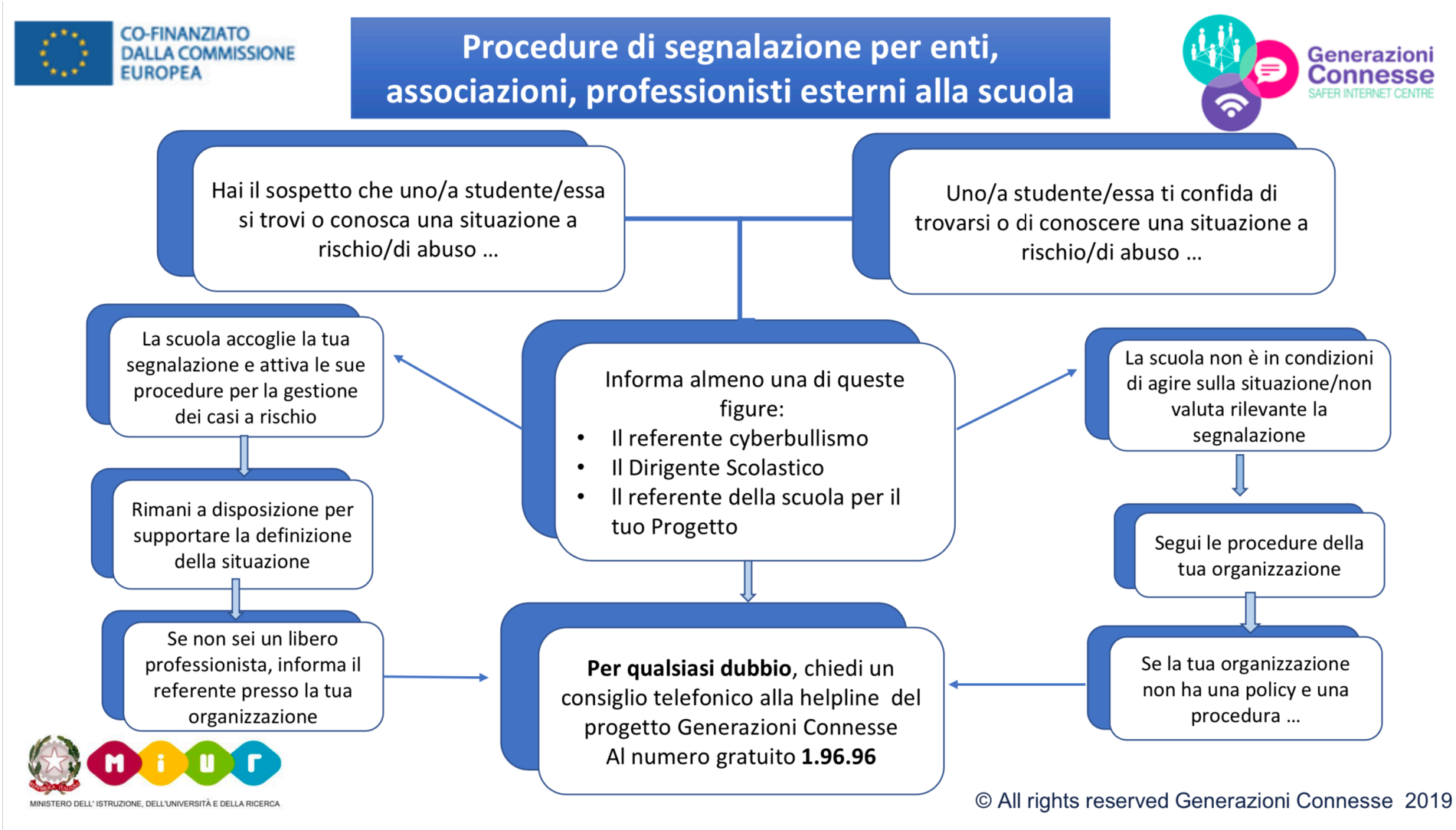
Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.
A) Se c'è fattispecie di reato - seguite le procedure della scuola
B) Se non c'è fattispecie di reato
- Richiedi la consulenza dello psicologo/a scolastico
- Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.
- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI
- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.
- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggerisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.
- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse
SAFER INTERNET CENTRE
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Rimani a disposizione per supportare la definizione della situazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Informa almeno una di queste figure:
• Il referente cyberbullismo
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Segui le procedure della tua organizzazione
Se la tua organizzazione non ha una policy e una procedura …
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019