Istituto Comprensivo "Ferraris" di Vercelli

Ministero dell'Istruzione, dell'Università e della Ricerca. Ufficio Scolastico Regionale per il Piemonte.

Scuola Statale Infanzia – Primaria – Secondaria 1° grado
Piazza Cesare Battisti, 6 - 13100 VERCELLI
Tel. 0161/257999 - Fax 0161/501543 C.F.94023410023 - Cod. VCIC810005

PEO: vcic810005@istruzione.it PEC: vcic810005@pec.istruzione.it URL: www.icferraris.gov.it

E-Safety Policy

I.C. Ferraris di Vercelli

1 INTRODUZIONE

a) Scopo della Policy.

b) Ruoli e Responsabilità.

c) Condivisione e comunicazione della Policy all'intera comunità scolastica.

d) Gestione delle infrazioni alla Policy.

e) Monitoraggio dell'implementazione della Policy e suo aggiornamento.

f) Integrazione della Policy con Regolamenti esistenti.

2 FORMAZIONE E CURRICOLO

a) Curricolo sulle competenze digitali per gli studenti

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

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

d) Sensibilizzazione delle famiglie.

3 GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

a) Accesso ad internet e Gestione accessi. E-mail.

b) Sito web della scuola

c) Social network.

d) Protezione dei dati personali.

4 STRUMENTAZIONE PERSONALE

a) Studenti

b) Docenti e altro personale

5 PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

a) Prevenzione, Rischi, Azioni

b) Rilevazione - Come segnalare: quali strumenti e a chi.

c) Gestione dei casi.

d) Definizione delle azioni da intraprendere a seconda della specificità del caso.

1 INTRODUZIONE

1.a Scopo della Policy.

L'uso delle tecnologie e di Internet è parte integrante sia della gestione della scuola sia del percorso educativo degli studenti. Le competenze Chiave delineate dal Parlamento Europeo prevedono lo sviluppo di competenze digitali e la scuola ha il compito di guidare gli studenti in tale percorso.

Internet è ormai fondamentale nella nostra vita, però è anche una potenziale fonte di rischi, tanto maggiori quanto meno si conoscano i modi legittimi di utilizzo e si abbia scarsa consapevolezza delle funzioni della rete.

La scuola permette di accedere ad Internet in molteplici modi:

1. computer a disposizione del personale ATA per la gestione amministrativa della scuola
2. computer messi a disposizione degli insegnanti
3. le LIM ormai presenti in tutte le classi
4. dispositivi mobili condivisi forniti dalla scuola
5. accesso al wi-fi della scuola sia per dispositivi privati dei docenti sia per dispositivi privati degli studenti (BYOD) soprattutto per le classi iPad.

Le norme che seguiranno forniscono agli utenti indicazioni per un uso corretto e generalizzato delle infrastrutture di rete (interna ed esterna).

Un utilizzo improprio di dispositivi e rete non solo può generare problemi di funzionalità di hardware e software, ma soprattutto rischia di produrre effetti dannosi per la sicurezza dei dati, il rispetto della privacy, il successo didattico e

formativo. Pertanto, il mancato rispetto di tali norme non è solo dimostrazione di imperizia tecnica, ma può far incorrere in reati sanzionabili.

Lo scopo della E-Safety Policy è:

1. stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie,
2. salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto;
3. assistere il personale della scuola permettendo di lavorare in modo sicuro e responsabile con le tecnologie di comunicazione;
4. impostare chiare aspettative di comportamento e fissare norme condivise per un uso corretto e responsabile di Internet a scopo didattico, personale o ricreativo;
5. prevenire e affrontare gli abusi online (come il cyberbullismo), in accordo con le altre politiche della scuola;
6. garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che, se si riscontreranno violazioni, saranno intraprese le opportune azioni disciplinari e giudiziarie.

È dunque importante definire all'interno dell'Istituto alcune regole chiare che permettano di lavorare in modo sereno e consentano di usare le tecnologie in modo efficiente e proficuo.

Questo documento costituisce parte integrante del **Regolamento di Istituto** e verrà portato a conoscenza dei genitori, degli studenti e di tutto il personale della scuola. Le norme di questo documento valgono per tutti gli spazi e laboratori dell'Istituto. Il personale interno all'Istituto (docenti, ATA e studenti) ed esterno (genitori, tirocinanti, esperti che collaborano con la scuola, ecc.) prende visione del presente documento, che sarà revisionato annualmente.

Il presente regolamento, da un punto di vista legislativo e amministrativo, è ispirato e promosso da direttive del Ministero dell'Istruzione a livello nazionale e regionale e fa costante riferimento alle norme legislative specifiche del settore.

1.b Ruoli e Responsabilità.

Dirigente scolastico

Il Dirigente Scolastico promuove le azioni necessarie per attuare le norme del presente regolamento, controllarne l'attuazione, irrogare le sanzioni,

comunicare con enti esterni alla scuola. Per questa attività si avvale anche della consulenza dell'animatore digitale e del Team per l'innovazione.

DSGA

Nei limiti dei bilanci, pianifica gli interventi tecnici e gli acquisti per garantire l'efficienza, la continuità e l'innovazione della scuola.

Garantisce inoltre la presenza e l'efficienza del registro elettronico dell'istituto.

Docenti

1. Pongono la massima cura che le password di accesso ai sistemi della scuola (registro elettronico e wi-fi) non siano conosciute dagli alunni.
2. Forniscono a tutti gli studenti una formazione sull'uso corretto di Internet e sui rischi della rete.
3. Illustrano il Regolamento di Istituto agli allievi spiegando quale utilizzo di dispositivi e di rete sia autorizzato dalla scuola.
4. I docenti che portano gli alunni nell'aula informatica illustrano, nel caso in cui gli alunni debbano accedere alla rete internet per la loro attività, le regole adottate dalla scuola e gli eventuali problemi che possono verificarsi.
5. Ricordano agli alunni che la violazione consapevole delle norme adottate dall'Istituto comporta sanzioni proporzionate alla gravità della violazione;
6. Non scaricano file video o musicali protetti da copyright;
7. Consultano animatore digitale e Team per l'innovazione prima di scaricare/installare software che ritengono utile.
8. Cercano di limitare al minimo l'uso di pendrive USB personali che devono collegare ai PC della scuola e, qualora ne facciano uso, si accertano che siano prive di virus o malware.

Personale scolastico

Vigila, di concerto con i docenti, che gli studenti non utilizzino telefoni cellulari per scopi personali e non autorizzati.

Alunni

Gli alunni nelle attività in cui utilizzano i PC e tablet della scuola o dispositivi privati per uso didattico:

1. non devono utilizzare giochi (o qualsiasi altro programma non autorizzato) né in locale né in rete;

2. devono riferire all'insegnante in caso di reperimento di immagini inappropriate od offensive durante la navigazione su Internet;
3. devono chiedere l'autorizzazione al Docente nel caso in cui, per svolgere un'attività in rete, occorra iscriversi , registrarsi e fornire dati personali;
4. devono chiedere al Docente il permesso prima di scaricare documenti dalla rete, e in ogni caso non scaricano file video o musicali protetti da copyright;
5. Non devono scaricare / installare sui PC della scuola software e devono chiedere l'autorizzazione ai docenti per scaricare file, che comunque non devono essere soggetti a copyright.
6. Devono limitare l'uso di pendrive USB e comunque devono chiedere al docente presente in aula il permesso di farne uso, assicurandosi a casa che siano privi di virus o malware.

1.c Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-Safety Policy d'istituto si applica a tutte le figure che possono avere accesso alle reti interne della scuola, quali personale docente e studenti, oppure che, come genitori, ne siano coinvolte nella vigilanza domestica.

La e-Policy di Istituto, come le altre documentazioni relative alla scuola, è pubblicata sul sito scolastico.

All'atto dell'iscrizione o all'inizio dell'anno scolastico la scuola chiede ai genitori degli studenti il consenso all'uso di Internet per i figli e per la pubblicazione dei loro lavori e delle loro fotografie sul sito e sulle pagine istituzionali. Patto di corresponsabilità e liberatorie sono inserite anche nel diario scolastico fornito gratuitamente alle famiglie di scuola primaria e secondaria.

Il personale e le famiglie sono consapevoli del fatto che sia sanzionabile una condotta non in linea con il codice di comportamento dei pubblici dipendenti e con la policy d'Istituto.

I genitori saranno informati della policy della scuola e saranno invitati, con metodi che saranno stabiliti, alla collaborazione con la scuola nel perseguire la sicurezza nell'uso di Internet.

La scuola pone particolare attenzione alle sviluppo di una "**cittadinanza digitale**" consapevole in modo che, per tutti, Internet possa essere un diritto ed una risorsa.

1.d Gestione delle infrazioni alla Policy.

L'utilizzo della rete interna/esterna (web) avviene all'interno della programmazione didattica e nell'ambito delle esigenze relative alle comunicazioni tra i plessi e la segreteria.

Il docente è il primo soggetto che favorisce l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e gestione della risorsa informatica. L'Istituto regolamenta l'uso dei laboratori indicando norme che consentono di vigilare sull'uso corretto dell'accesso ad Internet.

Disciplina degli alunni

A fronte di violazioni accertate delle regole stabilite dal presente regolamento si assumeranno i provvedimenti disciplinari previsti dal **Regolamento di Istituto**.

La violazione colposa o dolosa accertata delle norme del presente regolamento, oltre all'intervento disciplinare, potrà dare luogo alla richiesta di risarcimento dei danni e delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile.

Rimangono comunque applicabili ulteriori sanzioni disciplinari, eventuali azioni civili per danni, nonché l'eventuale denuncia del reato all'Autorità Giudiziaria.

La scuola prenderà le precauzioni necessarie per garantire la sicurezza on-line.

Non si può tuttavia escludere che durante la navigazione sui computer dell'Istituto o su dispositivi privati (BYOD) si trovi materiale non appropriato e/o indesiderato.

La scuola non può farsi carico in toto delle responsabilità per il materiale non idoneo trovato o per eventuali conseguenze causate dall'accesso al Web. Per tale ragione, gli utilizzatori devono essere pienamente coscienti dei rischi cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi (pornografia, violenza, razzismo ...).

Disciplina del personale scolastico

In caso di violazione colposa o dolosa accertata delle norme del presente regolamento, 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 gravita delle infrazioni commesse.

Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Nel caso di infrazione consapevole da parte dei docenti o del personale non docente, sarà in ogni caso compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

Disciplina dei genitori

È possibile che alcune condotte dei genitori o loro omissioni di vigilanza possano favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri. Appare opportuno ricordare che culpa in vigilando e culpa in educando potrebbero costituire elementi di valutazione.

1.e Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto ogni anno.

Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione di figure che si occupano dell'informatica nella scuola (animatore digitale, referente contro bullismo e cyberbullismo, referente salute, Team per l'innovazione, referente commissione PTOF).

1.f Integrazione della Policy con Regolamenti esistenti.

Il presente documento va ad integrare il Regolamento d'Istituto, la PUA, il PTOF e costituisce modello di riferimento per ulteriori regolamenti futuri.

2 FORMAZIONE E CURRICOLO

2.a Curricolo sulle competenze digitali per gli studenti

Una prima definizione di Competenze Digitali è stata proposta, nel 2006, dal Parlamento Europeo nel documento "Raccomandazione del Parlamento

Europeo e del Consiglio" del 18 dicembre 2006, che indicava le otto competenze chiave per l'apprendimento permanente: "la competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC (Tecnologie dell'Informazione e della Comunicazione): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".

Nel 2018 il Consiglio ha rivisto le Competenze Chiave e nella Raccomandazione del Consiglio del 22 maggio 2018, la Competenza Digitale è così definita:

"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".

Competenza digitale significa padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con autonomia, responsabilità, spirito critico e creatività, nel rispetto degli altri e sapendone prevenire ed evitare i pericoli.

In questo senso, **tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione**.

Il nostro Istituto da anni si avvale di interventi di Esperti (Polizia di Stato, Polizia locale, Polizia postale, Carabinieri, ASL, ARPA, ecc..) che operano attraverso incontri specifici rivolti ad alunni, docenti e famiglie e aventi come tematica il rispetto della Legalità, l'uso corretto delle nuove tecnologie e la salvaguardia della salute.

La nostra scuola è inoltre capofila provinciale nella prevenzione e nella lotta contro Bullismo e Cyberbullismo e dal 2014 sono attivi progetti di Peer Education (Gruppo Noi) che favoriscono non solo la formazione, ma anche un impegno diretto dei ragazzi.

Il nostro Istituto inoltre organizza tutti gli anni Eventi e Corsi di formazione aperti al territorio per sensibilizzare studenti, docenti, personale e famiglie su tali tematiche.

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

Il corpo docente ha partecipato a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze e, nel caso delle figure di sistema, anche di carattere specialistico. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica e sulla sicurezza on-line può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva all'interno dell'istituto e/o on-line, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo.

In seguito all'emergenza Covid19 si sono svolti incontri periodici di formazione online (con Hangouts Meet) o in modalità asincrona (tramite tutorial) coordinati dall'Animatore digitale e dal Team dell'innovazione per permettere a tutto il personale di gestire la DaD, padroneggiando gli strumenti a disposizione grazie alle Google Apps for Education e al registro elettronico.

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

Nell'anno scolastico 2019/2020, al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT, e di prevenire e contrastare "ogni forma di discriminazione e di cyberbullismo" (Legge 71/2017), il nostro Istituto ha aderito al progetto "Generazioni Connesse" (SIC: Safer Internet Center), coordinato dal MIUR.

Tale progetto prevede lo svolgimento di un Piano d'Azione che ha diversi ambiti di sviluppo, tra cui la formazione docente.

Inoltre il Referente contro Bullismo e Cyberbullismo, l'Animatore digitale e il Referente Salute seguono una formazione avanzata sulla piattaforma ELISA.

La Scuola si impegna inoltre ad organizzare le seguenti attività di prevenzione rispetto al fenomeno:

1. organizzazione di Corsi di formazione per docenti e genitori;
2. monitoraggio sul tema del cyberbullismo attraverso questionari;
3. formazione di tutti gli studenti su tale tematica e promozione della Peer Education con partecipazione volontaria al GRUPPO NOI

4. promozione della partecipazione di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo;
5. interventi di consulenza e supporto, relativamente a casi di bullismo e cyberbullismo.

2.d Sensibilizzazione delle famiglie.

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (E-Policy) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

3 GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

3.a Accesso ad internet e Gestione accessi.

L'istituto Comprensivo Ferraris è composto da:

La Scuola Secondaria di I Grado "L.Verga"

Le Scuole primarie Rodari e Galileo Ferraris

Le scuole dell'Infanzia Collodi e Collodi Bis

La Segreteria ha sede presso il plesso G. Ferraris in Piazza Cesare Battisti 6

Tutti i plessi sono collegati alla rete internet. L'accesso alla rete è di competenza del Comune dove sono ubicati i plessi. Tutti i plessi hanno una rete WiFi interna.

Ci sono molte differenze negli aspetti dell'informatica dei diversi plessi, dovuti a vari fattori; ciò comporta che l'approccio alla E-policy debba essere necessariamente diverso.

Ogni plesso ha a disposizione PC dedicati esclusivamente agli insegnanti e personale ATA.

Tutte le aule di ogni plesso di scuola primaria e secondaria ha a disposizione una LIM connessa alla rete dell'Istituto, utilizzata dagli insegnanti per la didattica. Le LIM non possono essere utilizzate dagli studenti senza la supervisione del docente.

Anche la scuola dell'infanzia è dotata di una LIM mobile per poter essere agilmente spostata nelle sezioni che ne hanno necessità.

La scuola Secondaria e le scuole Primarie hanno a disposizione laboratori informatici e/o dispositivi mobili condivisi che sono utilizzati per la didattica sotto la supervisione del docente e possono collegarsi alla rete dei singoli plessi.

La rete WiFi dei plessi è utilizzata dalle LIM, dai pc a disposizione di docenti e personale ATA, dai pc dei laboratori e dai dispositivi mobili della scuola, dai docenti per collegare i dispositivi privati e dagli studenti delle classi iPad per consentire il BYOD.

L'accesso al wi-fi della scuola permette di collegare un massimo di due dispositivi per utente e ogni utente è identificato tramite User-id e Password consegnata dal Dirigente scolastico.

Le apparecchiature informatiche della segreteria dell'istituto hanno una regolamentazione riservata e non è interessata dalla presente e-policy.

Le regole di base relative all'accesso ad Internet sono parte integrante del Regolamento d'Istituto, e sono esposte su apposita sezione del Sito della Scuola.

Sarà cura dei docenti illustrare i contenuti delle norme per l'utilizzo delle TIC agli studenti, tenendo conto della loro età ed evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica. Per l'utilizzo di laboratori e dispositivi comuni, sarà cura del responsabile di laboratorio e del docente che accompagna gli studenti in laboratorio o fornisce i dispositivi mobili non solo illustrare con cura la normativa, ma vigilare sul corretto e rispettoso utilizzo delle risorse della scuola.

I genitori saranno informati sulle E-policy d'istituto tramite la pubblicazione del regolamento sul sito web della scuola.

3.b E-mail.

I docenti di tutti i plessi e gli studenti della scuola Secondaria ricevono una mail istituzionale (nome.cognome@vergaferraris.net) con cui possono accedere ai servizi di **G-Suite for Education.**

Per ricevere tali credenziali il personale e le famiglie dovranno leggere e sottoscrivere il regolamento, il patto di corresponsabilità e le liberatorie previste dalla scuola, impegnandosi ad utilizzare tale servizio per scopi didattici e nel rispetto delle norme condivise.

La mail istituzionale fornita agli studenti permette di scrivere e ricevere mail o condividere materiale solo all'interno del dominio (@vergaferraris.net), pertanto ai fini esclusivamente didattici e sotto la supervisione del docente è consentito l'utilizzo di un indirizzo di posta elettronica personale (predisposto dalla famiglia per l'alunno). Tale eventualità può nascere da esigenze didattiche di utilizzo di piattaforme online, libri digitali o applicazioni che richiedono la registrazione di un account personale.

Le applicazioni utilizzate per la scuola saranno gratuite e accuratamente selezionate e testate dal docente prima di essere presentate agli studenti.

L'utilizzo della posta elettronica personale dovrà osservare le stesse regole di utilizzo presenti in questo documento per gli account di Istituto.

L'istituto non si ritiene responsabile di un eventuale utilizzo improprio dell'indirizzo e-mail personale da parte dello studente.

Il rapporto per l'uso della mail istituzionale coincide con la durata di permanenza nell'Istituto.

L'account verrà sospeso nel momento in cui lo studente non frequenterà più l'I.C. Ferraris e il docente non lavorerà più nell'Istituto. Sarà cura di docenti e studenti salvare eventuali dati personali su altri servizi cloud personali o su supporti esterni.

3.c Sito web della scuola

L'accesso al sito web di istituto (www.icferraris.edu.it) è libero, pertanto anche i materiali e i servizi disponibili per l'utenza (docenti, studenti e famiglie) sono liberamente fruibili e non viene richiesta alcuna password per la loro consultazione. Per materiale a carattere non di pubblico dominio, è prevista un'AREA RISERVATA per accedere alla quale occorre essere in possesso di credenziali forniti dalla scuola.

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni: consultazione elenchi libri di testo; PTOF; Regolamento di Istituto; informazioni generali sull'Istituto; informazioni sui progetti attivati dall'istituto; informazioni sull'amministrazione dell'istituto; albo di Istituto; avvisi e comunicazioni; moduli vari; circolari per i docenti; ed altro.

Sarà cura del responsabile della gestione delle pagine del sito della scuola vigilare che il contenuto sul sito sia appropriato. Per i documenti che si trovano sul sito viene chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

La scuola non pubblicherà materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi saranno pubblicate con il

consenso dei loro genitori. Le fotografie degli studenti per il sito della scuola saranno selezionate in modo tale che gruppi di alunni siano ritratti in attività didattiche a scopi documentativi.

Nel sito web della scuola è presente anche un collegamento "esterno" al registro elettronico, strumento on-line facente le funzioni di registro di classe e registro personale del docente con accesso con credenziali da parte dei genitori per valutazioni, note, programmi svolti, agenda, sezione didattica per scambio di materiali, bacheca. Il servizio di Registro on-line non viene gestito dall'Istituto, ma è fornito da una società esterna (Gruppo Spaggiari S.p.A). Tale piattaforma risiede su un altro server, pertanto essa risponde a criteri di policy non previsti dal presente documento.

L'Istituto si impegna a mantenere efficienti i servizi offerti, a migliorarli e estenderli nell'ottica di aumentare la qualità.

3.d Social network.

L'Istituto possiede una pagina facebook (@IstitutoComprensivoFerrarisVercelli)

La pagina Facebook di Istituto è gestita dall'animatore digitale sotto la supervisione del Dirigente scolastico.

Il materiale pubblicato ha lo scopo di mettere in luce progetti, attività, riconoscimenti di tutti i plessi della scuola. Previa liberatoria da parte delle famiglie, potranno essere pubblicate immagini degli alunni, privilegiando le visioni di insieme rispetto al primo piano di singoli.

3.e Protezione dei dati personali.

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l'ausilio di strumenti elettronici e comunque nel rispetto delle norme vigenti, in particolar modo il REGOLAMENTO EUROPEO PER LA PROTEZIONE DEI DATI (GDPR 25 MAGGIO 2018).

4 STRUMENTAZIONE PERSONALE

4.a Studenti

Nell'Istituto non è consentito agli alunni l'utilizzo di telefoni cellulari per scopi privati (se vengono portati a scuola, vanno tenuti spenti). In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno

comunicare con le famiglie tramite gli apparecchi telefonici della scuola, pertanto è indispensabile che le famiglie forniscano recapiti telefonici a cui possano essere facilmente reperibili.

Per quanto concerne l'utilizzo dei tablet o PC portatili (Attività BYOD – Bring your own device), potranno essere utilizzati solo se permessi dal docente, alla presenza del docente e per ragioni prettamente scolastiche.

Discorso a parte meritano le classi iPad, in cui l'utilizzo del dispositivo privato è parte integrante del percorso didattico scelto. Gli studenti avranno cura del proprio dispositivo che deve essere provvisto di un codice di blocco schermo in modo che non sia possibile ad altri accedere ai contenuti privati. Durante l'intervallo l'iPad deve rimanere in classe riposto con cura. In caso di uscita della classe, l'aula verrà chiusa a chiave dal personale per evitare danneggiamento colposo o intenzionale dei dispositivi, utilizzo non autorizzato e furti.

4.b Docenti e altro personale

Durante le ore di lezione è consentito ai docenti e al personale l'uso di cellulari, PC portatili e tablet di loro proprietà a scopo lavorativo, didattico e ad integrazione dei dispositivi scolastici disponibili (Attività BYOD – Bring your own device). Il docente, con il proprio User Id, potrà collegare al wi-fi della scuola fino a un massimo di due dispositivi, tuttavia, per non sovraccaricare la linea è preferibile che ogni docente colleghi un solo dispositivo.

5 PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5. a Prevenzione, Rischi, Azioni

Rischi

Gli insegnanti, per la natura stessa del loro lavoro, devono prevedere, prevenire e fronteggiare le problematiche e i rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.

Responsabilità degli insegnanti è, dunque, imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di:

1. bullismo/cyberbullismo (si veda quanto indicato nella legge 71 del 2017);
2. sexting: pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet;

3. adescamento o grooming: una tecnica di manipolazione psicologica, che gli adulti - potenziali abusanti - utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata;

I rischi che gli alunni possono correre a scuola derivano da un uso non corretto dei dispositivi elettronici, in particolare di quelli personali.

Azioni

Scuola e famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educhi all'accettazione, alla consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva. Anche nel guidare i ragazzi verso un uso corretto e responsabile di strumenti elettronici e di Internet è determinante un accordo educativo tra scuola e famiglia.

Occorre pertanto rafforzare e valorizzare il Patto di Corresponsabilità educativa.

La scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli, ma anche vigilando sui loro comportamenti.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti sono le seguenti:

1. Diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web.
2. Organizzare incontri con esperti (psicologo, Polizia Postale, Polizia locale ecc.) nelle singole classi o per l'intero Istituto e aventi per oggetto le tematiche del cyberbullismo, del sexting e dell'adescamento.
3. Organizzare corsi di formazione - in collaborazione con l'Asl e altri enti - ad ampio respiro, che non solo trattino dell'uso di dispositivi e internet, ma anche aiutino a riconoscere e gestire le emozioni e le tipologie di relazione (Patentino dello Smartphone, Diario della salute...)
4. Richiedere autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro).
5. Attento monitoraggio da parte del personale docente affinché il presente regolamento venga rispettato.

6. Tempestivo intervento tramite opportuna sanzione qualora il regolamento venga disatteso. Accanto alla sanzione, tuttavia, va proposto anche un percorso rieducativo perché solo attraverso l'educazione e il coinvolgimento di studenti e famiglie si possono correggere tali comportamenti devianti. La sola sanzione, non affiancata a un percorso educativo, ha scarsi effetti.

5.b Rilevazione - Come segnalare: quali strumenti e a chi.

Per episodi rilevabili tramite il telefono cellulare, ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Per le segnalazioni di fatti rilevanti si agirà conformemente a quanto stabilito nel Regolamento d'Istituto.

In caso di abusi sessuali, la denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. L'intervento dovrebbe riguardare gli ambiti medico, socio-psicologico e giudiziario.

Il compito della scuola è quello di prevenire l'abuso e, nel caso questo avvenga, di aiutare l'eventuale vittima, in quanto l'atto implica aspetti relazionali ed educativi che possono contribuire alla crescita serena del minore.

Per riuscire in questi intenti la scuola collabora con altre figure professionali e le famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo occasioni di confronto e di dialogo.

Di fronte ad azioni che violino il Regolamento di Istituto, le famiglie degli alunni vittime e di quelli responsabili saranno informate tempestivamente per un confronto.

In base all'entità dei fatti si provvederà a:

1. Una comunicazione scritta tramite diario alle famiglie;
2. Una nota disciplinare tramite registro elettronico;
3. Una convocazione formale dei genitori degli alunni, tramite segreteria;

4. Una convocazione delle famiglie da parte del Dirigente Scolastico o di suo delegato.

Per i fatti più gravi la scuola potrà rivolgersi direttamente agli organi di Polizia competenti.

L'uso sempre più capillare di strumenti digitali, classi virtuali, e attività digitali che, pur svolte a casa hanno una ricaduta anche sugli equilibri della classe (si pensi alla creazione dei gruppi classe su WhatsApp da parte degli alunni e alle complesse dinamiche relazionali al loro interno) rende più labile il confine tra ciò che può essere considerato un atto svolto all'interno o all'esterno della scuola.

Fatta tale premessa, la scuola ritiene ambito di propria competenza ciò che avviene all'interno dell'edificio scolastico o durante attività proposte dalla scuola (viaggi di istruzione, gare sportive studentesche, uscite sul territorio) o nelle classi virtuali create dai docenti, nelle mail istituzionali e durante le video conferenze. In tutti i casi in elenco, infatti, è prevista una supervisione da parte dei docenti.

Diverso è il discorso per quanto riguarda i gruppi whatsapp di classe, in cui non è presente il docente, ma sono comunque connessi all'attività scolastica. Per prevenire situazioni spiacevoli e disagi agli studenti la scuola si impegna a:

1. fornire una formazione agli studenti sui rischi di Internet e sull'uso improprio di chat e classi virtuali
2. condividere con gli studenti norme e regole di comportamenti virtuosi in rete (Netiquette) prendendo come base le indicazioni del progetto Parole-O-Stili e il decalogo della comunicazione Non Ostile.
3. Aiutare i ragazzi a concordare regole per il funzionamento sereno di gruppi chat; ciò li aiuterà non solo a gestire i gruppi whatsapp di classe in autonomia e con senso di responsabilità, ma permetterà loro di acquisire strumenti utili anche per il loro futuro.
4. Coinvolgere le famiglie qualora la scuola venga a conoscenza di comportamenti non corretti anche in ambiti di non diretta competenza
5. Qualora emergano difficoltà o comportamenti scorretti dedicare del tempo con la classe per riflettere e rielaborare l'accaduto, guidando i ragazzi nell'analisi della situazione con lo scopo di ricreare concordia e prevenire tensioni e disagi, o superarli qualora si siano già manifestati.

5.c Gestione dei casi.

Per quanto riguarda la gestione dei casi il nostro Istituto ha individuato una figura referente. La segnalazione del caso dovrà quindi essere fatta dal singolo docente al Referente per la prevenzione di Bullismo e Cyberbullismo, che si occuperà di raccogliere tutte le informazioni possibili e 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.

5.d Definizione delle azioni da intraprendere a seconda della specificità del caso.

Casi di cyberbullismo

(Il trattamento del Cyberbullismo è regolato dalle indicazioni della legge 71 del 2017; inoltre il nostro Istituto ha pubblicato un Opuscolo a riguardo distribuito alle scuole della provincia)

Si definiscono "bullismo" tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo, messi in atto con la volontà di danneggiare le vittime e si contraddistinguono per un evidente squilibrio di forza tra le parti.

Ben diverso è il caso del cyberbullismo, non solo perché la prepotenza viene attuata attraverso strumenti informatici, ma anche perché potenzialmente ognuno può facilmente passare dal ruolo di vittima a quello di bullo a quello di spettatore. L'anonimato, la distanza fisica, la natura stessa dello strumento che non necessita di una reiterazione volontaria dell'atto da parte del bullo (la reiterazione è automatica attraverso le visualizzazioni, i like, i commenti e le condivisioni) rendono il cyberbullismo molto più subdolo, più difficile da individuare da parte degli adulti e con conseguenze gravissime sulla vittima anche a distanza di molto tempo.

Il cyberbullismo ha infatti caratteristiche proprie.

1. Non è limitato a singoli ambienti: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo, anche tra le mura domestiche;
2. È un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo e, anche se cancellato, può ritornare;

3. Spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate;
4. Il cyberbullo spesso non è del tutto consapevole della gravità dei suoi comportamenti, se non viene aiutato a riconoscere le proprie responsabilità e valutare le conseguenze degli atti compiuti.

Qualora ci si trovi di fronte ad un caso di **cyberbullismo** (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà nel modo seguente.

- Il **docente** venuto a conoscenza del fatto dovrà:

1. Informare tempestivamente il referente;
2. Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di cyberbullismo;

A tale scopo si è predisposto un modulo condiviso all'interno di ogni Consiglio di Classe che permette di raccogliere le segnalazioni in modo ordinato (si veda Allegato 1)

- Il **referente** e il **CdC**

1. raccoglieranno tutte le informazioni possibili;
2. avviseranno il Dirigente scolastico
3. avviseranno le famiglie coinvolte
4. valuteranno, a seconda della gravità del caso, come sanzionare il/i responsabili (qualora sia stato possibile individuarli);
5. Proporranno agli studenti attività durante le quali questi possano confrontarsi sull'accaduto e rielaborare l'accaduto;

- Il **Dirigente** valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

Casi di sexting

Con il termine sexting si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite tramite cellulare o tramite internet.

Qualora ci si trovi di fronte ad un caso di sexting (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

Casi di adescamento online o grooming

Le tecnologie digitali consentono ai giovani di entrare in contatto con un enorme numero di persone sconosciute e spesso difficilmente identificabili. Non di rado gli adolescenti concedono la loro "amicizia" online non solo a persone che conoscono direttamente, ma anche ad "amici di amici" o a sconosciuti con cui vengono in contatto durante la navigazione e in particolare giocando online. Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.

L'adescamento online (grooming) consiste nel tentativo, da parte di un adulto, di avvicinare un bambino o adolescente, conquistandone la fiducia attraverso l'utilizzo della rete.

Gli insegnanti devono aiutare i propri alunni a riconoscere tali comportamenti e a tutelarsi, sia fornendo una formazione generale sia ascoltando i loro racconti e discutendo con loro di esperienze emerse.

Qualora il docente venga a conoscenza di situazioni potenzialmente o palesemente pericolose dovrà informare (come nei casi di Cyberbullismo) il Referente e il CdC che, raccolte tutte le informazioni, provvederanno a riferire al Dirigente e alla famiglia dell'alunno. Il Dirigente valuterà, come nei casi precedenti, se coinvolgere anche le autorità competenti.

Nota: tra il materiale consultato sul web al fine di trarre documentazione e modelli di riferimento, la E-Policy dell'I.C. Gaudenzio Ferrari di Momo (NO) ci ha fornito utili spunti di partenza.

ALLEGATO 1 I.C. Ferraris di Vercelli, Scuola _____ Classe _____ A.S. _____

Schema Riepilogativo delle situazioni gestite

Data	**Descrizione dell'episodio (specificando studenti coinvolti, docente che è venuto a conoscenza dei fatti…)**	**Azioni messe in atto**