



MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER LA LOMBARDIA

ISTITUTO COMPRENSIVO di NOVATE MEZZOLA

23025 NOVATE MEZZOLA (SO) - Via Ligoncio, n. 184 - C.F. 81002550143 - C.M. SOIC81600X

TEL: 0343/44126 MAIL: SOIC81600X@istruzione.it PEC: SOIC81600X@pec.istruzione.it SITO: www.icnovate.edu.it

E - P O L I C Y

USARE LE TECNOLOGIE IN SICUREZZA

Predisposto dal Team Antibullismo e dal Team Digitale

Approvato dal Collegio dei Docenti con delibera n. 30.2 del 19 febbraio 2025

Adottato dal Consiglio d'Istituto con delibera n. 22 del 15 maggio 2025



“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”

INDICE

1. CARATTERISTICHE DELL'E-POLICY.....	4
1.1. Condivisione	4
1.2. Integrazione con i Documenti esistenti	4
1.3. Aggiornamento e Monitoraggio	4
2. GESTIONE DELLE INFRAZIONI ALLA E-POLICY	5
3. RUOLI E RESPONSABILITÀ <i>per l'attuazione e la promozione dell'E-POLICY</i>	5
3.1. Dirigente Scolastico	5
3.2. Animatore Digitale	5
3.3. Referente bullismo e cyberbullismo	5
3.4. Docenti	6
3.5. Personale Amministrativo, Tecnico e Ausiliario (ATA)	6
3.6. Studenti e le Studentesse	6
3.7. Genitori	6
3.8. Enti educativi esterni e Associazioni	6
4. COMPETENZA DIGITALE, CURRICOLO E FORMAZIONE	7
4.1. La competenza digitale: conoscenze, abilità e atteggiamenti essenziali	7
4.2. La competenza digitale e curricolo d'Istituto	8
4.3. Competenza digitale e Formazione	8
5. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA E NELLA SCUOLA	8
5.1. Caratteristiche e Accesso alla rete informatica dell'Istituto	9
5.2. Utilizzo dei Laboratori, delle Postazioni e dei Software	10
5.3. Utilizzo Dominio, Piattaforme, E-Learning	10
5.4. Utilizzo Dispositivi Personali (BYOD)	11
6. PRINCIPALI RISCHI CONNESSI ALL'USO DELLE TIC	12
7. PRIVACY E SICUREZZA	13
8. CONCLUSIONI	14

P R E M E S S A

Le Tecnologie dell'informazione e della comunicazione (TIC) 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.*

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.

1. CARATTERISTICHE DELL'E-POLICY

Data la natura dei contenuti il presente documento non può che essere caratterizzato dalla massima condivisione, dalla integrazione con i documenti già presenti nella scuola, dall'aggiornamento costante e dal monitoraggio degli effetti prodotti dalla sua applicazione.

1.1. Condivisione

L'E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento. L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Viene redatta e condivisa con gli alunni una versione child friendly del documento per la comunicazione e la sensibilizzazione ai/le bambini/e e ai/le ragazzi/e.

L'E-Policy viene anche linkata nel modulo di autorizzazione all'uso della G Suite per gli studenti.

1.2. Integrazione con i Documenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

1.3. Aggiornamento e Monitoraggio

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il monitoraggio del documento prevede anche una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone:

- promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici;
- prevenzione e gestione dei rischi online.

2. GESTIONE DELLE INFRAZIONI ALLA E-POLICY

La scuola gestirà le infrazioni all'e-Policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità delle eventuali violazioni. Nei capitoli successivi del presente documento sono pertanto evidenziate le responsabilità di tutti gli attori della Comunità Educativa, elencati alcuni dei principali rischi connessi ad un uso poco consapevole delle tecnologie digitali e la disciplina del personale scolastico, degli studenti e delle studentesse, riguardante le possibili infrazioni nelle quali è possibile incorrere in caso di uso improprio dei device o della Rete informatica. Per quel che riguarda invece le infrazioni connesse al cyberbullismo, si rimanda al Regolamento Specifico dell'Istituto, contenente le infrazioni, le sanzioni e le procedure da attuare da parte di tutta la popolazione scolastica.

3. RUOLI E RESPONSABILITÀ *per l'attuazione e la promozione dell'E-POLICY*

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 nell'attuazione e promozione di essa.

3.1. Dirigente Scolastico

Si impegna per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. È formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove la cultura della sicurezza online e, insieme all'Animatore Digitale e al docente referente sulle tematiche del bullismo/cyberbullismo, propone corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Inoltre, il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

3.2. Animatore Digitale

Supporta il personale scolastico da un punto di vista non solo tecnico informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento anche allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati usino gli account forniti dall'Istituto e accedano alla Rete della scuola con apposita password solo per scopi istituzionali e consentiti (istruzione e formazione).

3.3. Referente bullismo e cyberbullismo

Ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo

non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori

3.4. Docenti

Hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Sono tenuti a integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti hanno il dovere di accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

3.5. Personale Amministrativo, Tecnico e Ausiliario (ATA)

Svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. È coinvolto nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA può essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

3.6. Studenti e le Studentesse

Si impegnano, in relazione al proprio grado di maturità e consapevolezza raggiunta, a utilizzare al meglio gli strumenti e le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

3.7. Genitori

In continuità con l'Istituto scolastico, devono essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; hanno il dovere di relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. Sottoscrivendo il patto di corresponsabilità, si impegnano ad accettare e condividere quanto scritto nell'e Policy dell'Istituto.

3.8. Enti educativi esterni e Associazioni

Gli enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

4. COMPETENZA DIGITALE, CURRICOLO E FORMAZIONE

La Raccomandazione del Consiglio europeo del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente (2018/C 189/01) individua le 8 competenze chiave per l'apprendimento permanente, definendo tra queste la competenza digitale. 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 cyber sicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.

4.1. La competenza digitale: conoscenze, abilità e atteggiamenti essenziali

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 cibersecurity), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.

Rispetto a tale competenza le persone dovrebbero:

- comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all'innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi;
- comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione, oltre a conoscere il funzionamento e l'utilizzo di base di diversi dispositivi, software e reti;
- assumere un approccio critico nei confronti della validità, dell'affidabilità e dell'impatto delle informazioni e dei dati resi disponibili con strumenti digitali ed essere consapevoli dei principi etici e legali chiamati in causa con l'utilizzo delle tecnologie digitali;
- essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l'inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali;
- avere la capacità di utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali;
- essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.

Interagire con tecnologie e contenuti digitali presuppone un atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Impone anche un approccio etico, sicuro e responsabile all'utilizzo di tali strumenti.

4.2. La competenza digitale e Curricolo d'Istituto

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo con maggiore “competenza”. Per questo la scuola si impegna a portare avanti percorsi volti a promuovere le competenze digitali, e l’uso consapevole e responsabile delle tecnologie digitali. Nel curricolo Digitale adottato dalla scuola è previsto e l’uso della Suite di Google secondo le modalità specificate più avanti nonché, tenendo conto degli obiettivi previsti dal Piano Scuola Digitale (PNSD), e dal DigComp 2.1 e 2.2 e della definizione di competenza digitale delle Raccomandazione del Consiglio europeo lo sviluppo delle competenze nelle seguenti aree:

Area 1: “Alfabetizzazione e dati”.

Area 2: “Comunicazione e collaborazione”.

Area 3: “Creazione di contenuti digitali”.

Area 4: “Sicurezza”.

Descrittori, livelli di padronanza e modalità valutative sono specificati nel Curricolo d'Istituto.

4.3. Competenza digitale e Formazione

È fondamentale che i docenti tutti siano formati ed aggiornati sull’uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo. Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti. La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento. Pertanto l’Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l’aiuto dell’animatore digitale), dalle reti di scuole e dall’amministrazione, sia quelle liberamente scelte dai docenti (anche online) sulle TIC e si impegna a organizzare ogni anno momenti di formazione sui metodi e sugli strumenti della didattica digitale nonché sull’uso consapevole e sicuro della rete.

5. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA E NELLA SCUOLA

Le apparecchiature e le risorse digitali presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.

Il Piano Nazionale della Scuola Digitale (PNSD) introduce l’utilizzo degli strumenti digitali da parte degli insegnanti e da parte degli alunni. Il PNSD 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. Gli utenti, siano essi maggiorenni o minori, 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; pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti: è dovere della Scuola garantire il diritto dei minori all'accesso alla rete e adottare allo stesso tempo tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio nella navigazione. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di stabilire regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose. Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti, o al reperimento ed uso di materiali inappropriati. Nell'uso delle Tecnologie dell'informazione e comunicazione, gli studenti si impegnano a:

- utilizzare la rete nel modo corretto;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità rimovibili personali;
- non utilizzare il telefono cellulare a scuola;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

gli docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

5.1. Caratteristiche e Accesso alla rete informatica dell'Istituto

1. L'infrastruttura di rete nell'istituto è costituita in tutti i 9 plessi da una doppia rete WIFI:
 - Rete WIFI IcNovate-Didattica = a cui sono connessi tutti i pc di classe, le LIM della scuola e tutti i dispositivi mobili dei laboratori (Chromebook o notebook a seconda della sede);
 - Rete WIFI IcNovate-Ospiti = a cui sono connessi temporaneamente (tramite l'erogazione, da parte del Team Digitale, di voucher temporanei) i device personali dei docenti o di persone esterne all'Istituto stesso.
2. Nel plesso principale di Novate Mezzola è presente una Rete LAN a cui è connessa la segreteria.
3. 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.
4. Internet non può essere usato per scopi vietati dalla legislazione vigente.
5. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet e per eventuali danni causati all'hardware e al software.
6. È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.
7. Tutti gli utenti connessi alla rete devono aderire alla legislazione vigente applicata anche alla comunicazione su internet.

8. I docenti possono richiedere la password di accesso alla rete wi-fi per finalità solo ed esclusivamente didattiche e non personali; è possibile profilare tablet e/o PC, escluso lo smartphone.
9. La password d'accesso alla rete wi-fi può essere richiesta rivolgendosi a chi ne è responsabile.
10. Ogni tentativo di forzare o manomettere la rete dell'Istituto e le sue protezioni sarà sanzionato come grave infrazione disciplinare.

5.2. Utilizzo dei Laboratori, delle Postazioni e dei Software

1. I docenti e gli studenti non devono installare software sulle macchine, senza prima aver interpellato il personale responsabile.
2. È vietato usare dispositivi e periferiche di archiviazione personale (penne USB e hard disk esterni), ma usare gli strumenti cloud messi a disposizione dall'Istituto (Drive).
3. Tutte le attività didattiche con strumenti digitali devono essere svolte solo ed esclusivamente nei laboratori informatici o usando i laboratori mobili.
4. Gli studenti per attività di studio, di ricerca e di approfondimento possono utilizzare i PC dei laboratori di informatica solo se autorizzati e accompagnati dai docenti. Possono anche usufruire di questi strumenti in orario extrascolastico, precedentemente fissato, solo se presentano formale richiesta.
5. L'accesso ai laboratori informatici è consentito solo ed esclusivamente per finalità didattiche, previa prenotazione attraverso l'apposita funzione presente sul registro elettronico.
6. I docenti che accompagnano gli studenti nei laboratori sono responsabili di eventuali danni causati alle macchine dagli studenti stessi e sono pregati di segnalare immediatamente il danno.
7. I docenti che accompagnano gli studenti nei laboratori, al termine delle attività devono accertarsi che tutte le macchine vengano spente e che le aule siano lasciate in ordine.
8. L'accesso ai PC delle aule è consentito solo ed esclusivamente ai docenti con le credenziali intranet.
9. Alla fine della lezione ogni docente è tenuto a disconnettere il proprio account dalla rete, eventualmente utilizzato.
10. Gli studenti possono utilizzare i PC solo se autorizzati dal docente e sotto la sua supervisione.
11. Il docente dell'ultima ora di lezione è tenuto a chiudere la postazione.
12. L'accesso ai PC è consentito solo ed esclusivamente ai docenti con le credenziali intranet.
13. Gli studenti non hanno accesso alle postazioni.

5.3. Utilizzo Dominio, Piattaforme, E-Learning

1. I docenti per le proprie attività didattiche e per la gestione della documentazione devono munirsi di un account del dominio @icnovate.edu.it forniti dal team digitale per l'innovazione; con tale account è possibile utilizzare tutti gli applicativi di G Suite for Education.
2. Tali domini devono essere utilizzati solo ed esclusivamente per le attività didattiche, le procedure di gestione della documentazione, la comunicazione con gli altri soggetti dell'Istituto e la comunicazione verso terzi sempre per attività inerenti alla Scuola.
3. Quando un docente cambia scuola può chiedere agli amministratori la migrazione dei propri dati su un altro account, altrimenti gli account saranno sospesi e dopo due anni eliminati.

4. Anche per gli studenti è previsto un account nel dominio @icnovate.edu.it dell'Istituto, sarà cura del Team digitale per l'innovazione profilare gli alunni e comunicare le credenziali di accesso attraverso il docente coordinatore di classe.
5. L'accesso agli applicativi di G Suite for Education da parte degli alunni, in particolar modo della scuola primaria, deve avvenire solo ed esclusivamente sotto la vigilanza dei docenti a scuola e dei genitori a casa.
6. Attraverso l'applicazione Google Classroom, l'insegnante crea, per ciascuna disciplina di insegnamento, un corso, inserendo i rispettivi alunni e avendo cura di invitare gli eventuali insegnanti di sostegno contitolari della classe. Per la scuola primaria si potrà creare una Classroom con tutti i docenti della classe.
7. Facendo ricorso ai vari applicativi della G-Suite for Education, i docenti gestiscono all'interno dei propri corsi le attività monitorando la partecipazione e i livelli di apprendimento degli alunni.
8. In questo contesto, è necessario prevedere frequenti momenti di interazione tra docenti e alunni, in modo da permettere la restituzione da parte degli insegnanti del senso di quanto operato in autonomia dagli alunni.
9. Estensioni e applicazioni in grado di aggiungere funzionalità e strumenti utili alla didattica possono essere affiancate ai servizi di base della G-Suite for Education.
10. Le consegne relative alle attività sulla piattaforma sono assegnate dal lunedì al venerdì, entro le ore 14:00 per consentire agli studenti di organizzare la propria attività di studio, lasciando alla scelta personale della studentessa o dello studente lo svolgimento di attività di studio autonoma anche durante il fine settimana.
11. Le consegne per lo svolgimento di un compito devono essere date all'alunno almeno con due giorni di anticipo.
12. L'invio di materiale didattico in formato digitale è gestito dal docente, il quale tiene conto del diritto alla disconnessione dello studente, pertanto non si inviano materiali il fine settimana e dopo le ore 17:00.
13. I docenti usano il registro elettronico con puntualità e tempestività, con particolare riferimento alla firma dei compiti e delle valutazioni.
14. I docenti annoteranno sul registro elettronico quotidianamente le attività svolte e inseriranno nella sezione "Agenda" i compiti, dopo aver provveduto a farli annotare sul diario agli alunni.
15. Ciascun docente, nell'ambito della propria libertà di insegnamento, può integrare l'uso delle piattaforme istituzionali con altre applicazioni web che consentano di documentare le attività svolte, sulla base delle specifiche esigenze di apprendimento delle studentesse e degli studenti.

5.4. Utilizzo Dispositivi Personali (BYOD)

1. In virtù della normativa vigente posta a tutela della privacy, è fatto divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire, divulgare e/o pubblicare immagini, filmati o registrazioni vocali senza il consenso esplicitamente espresso in forma scritta dagli interessati o i loro tutori (nel caso di minori).
2. È assolutamente vietato agli alunni l'utilizzo in classe del telefono cellulare, anche a fini educativi e didattici salvo i casi in cui lo stesso sia previsto dal PEI o dal PDP, ovvero per documentate e oggettive condizioni personali.

3. L'uso dello smartphone per i docenti, durante l'orario di lavoro, è consentito solo per motivi didattici e di servizio.
4. L'uso dello smartphone per il personale ATA, durante l'orario di lavoro, è consentito solo per motivi di servizio.
5. L'uso dello smartphone non conforme alle regole adottate nel presente Regolamento sarà sanzionato:
 - per gli studenti con i provvedimenti previsti dal Regolamento di Disciplina d'Istituto;
 - per il personale docente e non docente dal Dirigente scolastico, attraverso provvedimento di contestazione.
6. Con gli smartphone non è possibile utilizzare la rete WI-FI dell'Istituto.
7. I docenti e il personale ATA possono usare tablet e PC personali durante le ore di lezione e di servizio solo per finalità didattiche o di servizio.
8. Gli studenti, possono usare tablet e PC personali durante le ore di lezione solo per fini didattici, sotto la guida dei docenti.
9. I docenti controllano in classe il corretto utilizzo di PC e Tablet personali da parte degli studenti.

5.5. Aspetti disciplinari relativi all'utilizzo degli strumenti digitali

1. Gli studenti, i docenti, i genitori e il personale scolastico vengono informati del fatto che l'utilizzo dei supporti digitali e di Internet è costantemente monitorato dal personale responsabile, che ha accesso remoto agli account personali, inoltre vengono date loro istruzioni per un uso responsabile e sicuro. In particolare il controllo dei domini permette di individuare tutti gli eventuali abusi, occorsi prima, durante e dopo ogni sessione di lavoro.
2. In particolare, è assolutamente vietato diffondere sulle piattaforme in dotazione all'Istituto immagini o registrazioni relative alle persone e utilizzare gli strumenti digitali per produrre e/o diffondere contenuti osceni o offensivi.
3. Il mancato rispetto di quanto stabilito nel presente Regolamento, in particolare nei precedenti commi di questo articolo:
 - a) da parte delle studentesse e degli studenti può portare all'attribuzione di note disciplinari e all'immediata convocazione a colloquio dei genitori, e, nei casi più gravi, all'irrogazione di sanzioni disciplinari, compresa la sospensione dalle lezioni;
 - b) da parte del personale scolastico comporta l'avvio di un procedimento disciplinare e, nel caso in cui si ravvisino ipotesi di reato, la segnalazione all'autorità giudiziaria;
 - c) da parte del personale esterno, che collabora con l'Istituzione scolastica, comporta l'immediata sospensione della fruizione del servizio e, nel caso in cui si ravvisino ipotesi di reato, la segnalazione all'autorità giudiziaria.

6. PRINCIPALI RISCHI CONNESSI ALL'USO DELLE TIC

Per tantissimi adulti e ragazzi l'uso della tecnologia in modo sistematico è la normalità, tuttavia non sempre colgono le implicazioni dei loro comportamenti e questo avviene ancor più facilmente al diminuire dell'età. Non sempre i pericoli vengono percepiti come tali. Di seguito vengono riportati i principali, ricordando che è compito degli adulti, docenti e genitori, guidare i ragazzi a saperli

riconoscere ed evitare.

- esposizione a contenuti violenti o non adatti alla loro età;
- diffusione in rete di dati personali;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;
- furto di identità o di credenziali informatiche;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

7. PRIVACY E SICUREZZA

“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”.

7.1. Accesso persone esterne alle risorse di rete

1. È assolutamente vietato l’accesso a persone esterne ai dispositivi e alla rete dell’Istituto, ogni violazione sarà punita in termini di legge.
2. Le persone esterne all’Istituto possono accedere ai dispositivi digitali e alla rete solo in modalità Guest, dopo essere stati autorizzati dal Dirigente o dal personale responsabile.
3. Le persone esterne, che utilizzano i dispositivi digitali e dell’Istituto, sono responsabili di eventuali danni arrecati e di un uso illegale di essi.
4. Le persone esterne che utilizzano dispositivi digitali e rete dell’Istituto vengono informati del fatto che l’utilizzo dei supporti digitali e di Internet sono monitorati dal personale responsabile e vengono date loro istruzioni per un uso responsabile e sicuro.

7.2. Diritto alla privacy e autorizzazione per l’iscrizione degli studenti al dominio e alla piattaforma

1. L’iscrizione degli studenti al dominio e alla piattaforma è autorizzata dai genitori attraverso la compilazione del modulo allegato al diario scolastico d’istituto.
2. Ai genitori e/o tutori è richiesta all’inizio dell’anno scolastico (attraverso modulo allegato al diario scolastico d’istituto) un’autorizzazione alla pubblicazione della documentazione multimediale, da utilizzare a scopo documentario, didattico e scientifico e senza fini di lucro, in

qualunque forma o modo, in Italia o all'estero, senza limitazione di spazio e di tempo e senza compenso.

3. È diritto dei genitori e/o tutori rifiutare tale autorizzazione.

8. CONCLUSIONI

Le regole relative all'accesso ad Internet e agli strumenti digitali sono predisposte dal Team Antibullismo in Collaborazione con il Team Digitale, approvate dal Collegio dei Docenti e adottate dal Consiglio d'Istituto, vengono quindi attuate negli spazi dell'Istituto. Il personale scolastico riceve una copia del Regolamento, che va osservato scrupolosamente. Tutto il personale scolastico, pertanto, è coinvolto nel monitoraggio dell'utilizzo dei supporti digitali e di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sul loro uso sicuro e responsabile. L'E-Policy è parte integrante del Regolamento di Istituto e viene affisso all'Albo della Scuola e pubblicata nel sito web della scuola. Il Dirigente scolastico ha il diritto di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (tablet, notebook, ecc.) a chi non si attiene alle regole stabilite. I genitori/tutori vengono informati della pubblicazione dell'e-Policy della scuola e possono richiederne una copia.