



Ministero dell'Istruzione e del Merito

Liceo Statale "M. G. Agnesi"

Liceo Scientifico - Liceo Scientifico con opzione Scienze Applicate

Liceo Linguistico

Via dei Lodovichi 10 – 23807 Merate (LC) - Tel: 039 9906676-039 9902139

e-mailuffici: lcps020004@istruzione.it

E-SAFETY POLICY

Il Liceo Statale "M.G. Agnesi", in base alle linee guida delle politiche nazionali, ha elaborato una Policy di e-safety (Uso Accettabile e Sicuro di internet e le LAN - reti locali e device).

Verrà revisionata e aggiornata annualmente, anche in base ad eventuali variazioni delle dotazioni tecnologiche e dei protocolli dell'Istituto.

SOMMARIO

- 1. Introduzione**
- 2. Formazione e curriculum**
- 3. Utilizzo consapevole di internet**
- 4. Intelligenza artificiale e suo utilizzo**
- 5. Gestione infrastrutture e strumentazioni**
- 6. E-mail istituzionali**
- 7. Prevenzione**
- 8. Linee guida**
- 9. Didattica a distanza**

1. INTRODUZIONE

Le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte della regolare, abilitante, quotidiana attività scolastica, sono utilizzate nella comunicazione scuola-famiglia e rivestono un ruolo importante nella vita sociale degli alunni.

La presenza e l'utilizzo delle tecnologie digitali nella vita e nella didattica offre grandi possibilità, ma impone una riflessione sui rischi ad essa connessi e rende necessario sviluppare nuove competenze digitali sia per le nuove generazioni che per gli adulti.

Data la pervasività di tali tecnologie la scuola è perciò chiamata a redigere norme di comportamento alle quali tutti i membri della comunità scolastica sono chiamati ad attenersi al fine di garantire un ambiente sicuro, nonché ad attivare percorsi di formazione per promuovere un uso consapevole e responsabile della rete stessa.

SCOPO DELLA E-SAFETY POLICY

- Informare l'utenza per un uso corretto e responsabile delle apparecchiature e delle piattaforme informatiche.
- Promuovere l'uso consapevole e critico da parte degli alunni, dei docenti e del personale delle tecnologie digitali e di internet.
- Prevenire e fronteggiare le problematiche che derivano da un utilizzo non responsabile, lesivo o dannoso, delle tecnologie digitali.
- Definire un codice di comportamento impostando delle regole di condotta chiare per un uso consapevole e critico di internet, dei device pubblici e dei dispositivi privati in ambiente didattico, regolamentandone le infrazioni.

CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

La policy sarà condivisa con alunni, personale della scuola e genitori attraverso il presente documento, riunioni informative, corsi di formazione specifici all'interno o all'esterno dell'istituto.

La scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato delle TIC e limitato alle esigenze didattiche.

Il coinvolgimento dei genitori sul tema della sicurezza nell'uso delle tecnologie digitali e di internet sarà pubblicizzato tramite il sito web della scuola.

2. FORMAZIONE E CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

La scuola ha inserito nel PTOF numerosi richiami alle competenze digitali per gli alunni, trasversali alle discipline previste dalle Indicazioni Nazionali.

La competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. *"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: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".*

Viene posta, perciò, l'attenzione sulla capacità di affrontare in modo flessibile le situazioni tecnologicamente nuove, analizzando, valutando e selezionando dati e informazioni in modo critico, sapendo individuare e sfruttare punti di forza e opportunità offerte dalle TIC, e sviluppando una responsabilità sociale.

In merito, la scuola delinea azioni per l'uso attento degli strumenti online al fine di garantire che siano adeguati all'età dei ragazzi e sostiene gli obiettivi di apprendimento in aree curriculari

specifiche individuate dai docenti; docenti ed alunni devono informarsi sui problemi di plagio o copyright; verrà insegnato agli alunni che non devono pubblicare immagini, registrazioni audio o video di altri senza permesso. Verranno spiegati i rischi connessi al fornire informazioni attraverso le immagini (tra cui il nome del file), che rivelano l'identità degli altri e la loro posizione. Impareranno la necessità di mantenere i loro dati sensibili al sicuro e cosa fare se sono oggetti di stalking o abusi.

Il corpo docente partecipa a corsi di formazione interni, esterni e nell'ambito di piani nazionali (PNSD) ed è disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.

3. UTILIZZO CONSAPEVOLE DI INTERNET

Gli utenti devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete.

Al fine di tutelare il rispetto normativo degli utilizzi di internet e dell'accidentale contatto con materiale inadeguato e/o illegale nonché di non rispettare il copyright, la Scuola promuove l'adozione di strategie che limitino l'accesso a siti illeciti.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta e favorire lo sviluppo delle competenze digitali degli studenti in relazione ad un corretto utilizzo ad una revisione critica delle fonti.

AREE DI RISCHIO PER LA COMUNITA' SCOLASTICA

Contenuti

- Esposizione a contenuti non appropriati (es. pornografia, accesso a siti vietati e/o non adeguati ecc.).
- Siti web che promuovono stili di vita e comportamenti dannosi (es. siti che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).
- Contenuti che spingono all'odio, al razzismo, all'intolleranza e alla violenza.
- Validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online e rispettare il copyright.

Contatto

- Grooming (adescamento online), sfruttamento sessuale.
- Cyberbullismo e bullismo in tutte le forme.
- Il furto di identità, comprese le password.
- Pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone reali e/o virtuali minorenni).

Condotta

- I comportamenti aggressivi (bullismo).
- Violazione della Privacy, tra cui la divulgazione di informazioni personali o di dati (foto, video, voce) senza autorizzazione dei soggetti interessati.
- Reputazione digitale.
- Salute e benessere: dipendenza da Internet e quantità di tempo speso online (Internet Addiction), gioco d'azzardo o gambling, videogiochi online in comunità mondiali.
- Sexting.
- Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore).

SENSIBILIZZAZIONE DELLE FAMIGLIE

L' Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete,

promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine verranno favoriti gli incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati, dall'ASST di Lecco e dalle forze dell'ordine.

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari o smartphone e delle chat o dei social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

4. INTELLIGENZA ARTIFICIALE E SUO UTILIZZO

ISTRUZIONE OPERATIVE E STRUMENTI DI ACCOMPAGNAMENTO

Come da Linee guida ministeriali per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche (*versione 1.0, anno 2025, Allegato al DM n. 166 del 09/08/2025*), prima di introdurre sistemi di IA il Liceo si propone di analizzare e valorizzare il proprio contesto scolastico, individuando i bisogni specifici e le aree di applicazione strategiche. Tale processo deve garantire il rispetto dei seguenti principi di riferimento (*si veda il capitolo 2 delle linee guida*):

- Centralità della persona
- Equità
- Innovazione etica e responsabile
- Sostenibilità
- Tutela dei diritti e delle libertà fondamentali
- Sicurezza dei sistemi e modelli di IA

Ai fini dell'integrazione dell'Intelligenza Artificiale all'interno di un'area considerata strategica si renderà quindi necessario coinvolgere e prestare ascolto alla comunità scolastica nell'identificazione di una necessità o di un'idea progettuale. Se quest'ultima è ritenuta valida e coerente con il Piano Triennale dell'Offerta Formativa (PTOF), saranno attivati gli organi collegiali, ciascuno per la propria competenza per la valutazione e, successivamente, l'approvazione formale del progetto.

Sarà poi necessario definire un piano di progetto che descriva la gestione del progetto, includendo la definizione di *milestone* e i connessi risultati attesi, il *team* coinvolto e i ruoli per ciascun attore, un piano dei costi e le modalità di monitoraggio del raggiungimento delle *milestone*. Dovrà inoltre essere definito un piano di gestione dei rischi che identifichi i potenziali rischi connessi al progetto, anzitutto in relazione alla tutela dei diritti e delle libertà fondamentali dei soggetti che interagiscono con i sistemi di IA (tutela della privacy, sicurezza dei dati e dei sistemi, possibilità di errori sistemici e discriminazioni anche solo involontarie, eventuali malfunzionamenti tecnici o problematiche legate alla trasparenza e all'utilizzo improprio degli strumenti).

Durante la fase di implementazione, alla luce della novità che rappresenta un sistema di IA, l'approccio dovrà essere graduale per poterne valutare gli esiti e solo successivamente si definiranno le modalità di estensione all'intero contesto scolastico. Il processo di transizione all'innovazione dovrà inoltre essere accompagnato da iniziative di comunicazione, informazione e formazione all'utilizzo consapevole ed efficace dei nuovi sistemi. Tale piano dovrà delineare gli obiettivi della strategia comunicativa, identificare gli *stakeholder* di riferimento e selezionare i canali di comunicazione più adeguati, avviando iniziative di comunicazione specifiche durante le principali fasi progettuali – lancio, gestione e conclusione.

Nella fase di monitoraggio si guarderà sia all'avanzamento e al raggiungimento delle *milestone* di progetto, sia ad anomalie, risultati inattesi o violazione di dati personali (da segnalare all'autorità di controllo).

Al termine delle attività, il progetto dev'essere sottoposto ad una valutazione interna del raggiungimento degli obiettivi e dell'analisi dei risultati rispetto al piano iniziale.

AREE DI APPLICAZIONE PER TIPOLOGIA DI DESTINATARI

Il Dirigente Scolastico, grazie all'aiuto di sistemi di Intelligenza Artificiale, può potenziare i necessari processi di analisi che supportano le decisioni.

L'IA può essere un prezioso supporto per il DSGA ed il personale ATA, ottimizzando i processi ripetitivi, migliorando l'efficienza e riducendo significativamente l'errore umano. Le attività di gestione amministrativa, comunicazione e organizzazione, che tradizionalmente richiedono un notevole impegno manuale, possono essere ottimizzate attraverso l'implementazione di tecnologie avanzate.

L'Intelligenza Artificiale, se ben utilizzata, può supportare le attività del personale docente, offrendo strumenti che semplificano e potenziano la preparazione e l'organizzazione della didattica. L'IA può offrire un supporto mirato alla didattica, creando percorsi formativi su misura e rendendo il processo educativo più coinvolgente e in linea con le esigenze individuali. Inoltre, l'IA permette di ampliare e diversificare l'offerta formativa, adeguandola alle esigenze e agli interessi degli studenti e supporta nella creazione di materiali didattici personalizzati che arricchiscono il percorso educativo.

Le applicazioni dell'IA a supporto degli studenti sono molteplici. L'IA può offrire un supporto mirato alla didattica, rendendo il processo educativo più coinvolgente e creando percorsi formativi su misura, in linea con le esigenze individuali e con quanto previsto dalle Linee guida per l'insegnamento dell'educazione civica in materia di competenze di "Cittadinanza digitale. Per sfruttare a pieno i benefici di queste tecnologie, è necessario garantire una formazione adeguata che aiuti gli studenti a utilizzare l'IA in modo consapevole, etico e sicuro. Gli studenti devono essere preparati a diventare co-creatori attivi di contenuti con l'IA, nonché futuri *leader* che definiranno il rapporto di questa tecnologia con la società.

MITIGAZIONE DEI RISCHI

L'introduzione dell'IA all'interno dell'Istituto comporta dei rischi che devono essere adeguatamente valutati per consentire una modalità di applicazione etica e corretta. Il Dirigente Scolastico e le figure di riferimento da lui preposte devono quindi assicurarsi che vengano attuate le seguenti azioni per limitare i rischi legati all'implementazione dell'IA:

- **Protezione dei dati:** l'adozione di misure di sicurezza per la gestione dei dati, insieme alla verifica che i sistemi utilizzati siano progettati secondo i principi di *privacy by design* e *by default*, garantisce il corretto trattamento delle informazioni personali in conformità con le normative sulla protezione dei dati. Occorre, inoltre, stabilire limiti ben definiti in merito all'accesso e all'uso dei dati raccolti, ponendo particolare attenzione all'impatto che tali operazioni possono avere sugli interessati, al fine di tutelarne efficacemente i diritti e la privacy.
- **Programmi di manutenzione:** l'implementazione di un piano di manutenzione regolare deve includere aggiornamenti costanti di *software* e *hardware*, monitoraggio continuo delle reti per risolvere tempestivamente eventuali problemi, *backup* periodici dei dati per evitare perdite, test di compatibilità per prevenire conflitti con nuovi aggiornamenti e formazione del personale scolastico per gestire e risolvere i problemi tecnici di base.
- **Progettazione etica degli algoritmi:** la definizione di un approccio proattivo nella progettazione e nello sviluppo degli algoritmi di IA, che includa l'*auditing* dei dati di addestramento per individuare e correggere eventuali *bias*, l'esecuzione di test regolari per garantire equità, il monitoraggio continuo e la normalizzazione dei dati, assicura che l'IA operi nel rispetto dei principi di non discriminazione e integrità etica. È inoltre fondamentale che la fase di addestramento contempli adeguate garanzie a tutela degli interessati, favorendo, ove possibile, l'utilizzo di dati sintetici in luogo di dati reali, al fine di minimizzare i rischi legati alla privacy e proteggere i dati personali sensibili.
- **Migliore comprensione dell'IA:** l'adozione di tecniche di spiegabilità dell'AI aumenta la trasparenza dei modelli, rendendoli più comprensibili e interpretabili. Poiché la fiducia nell'IA dipende dalla sua affidabilità, queste tecniche includono l'uso di algoritmi che forniscono

spiegazioni chiare e dettagliate delle loro decisioni, permettendo agli utenti di capire come e perché vengono prese determinate scelte e pianificando, se necessario, piani di emergenza;

- **Formazione continua:** una formazione specifica sull'uso responsabile dell'IA a tutto il personale favorisce un'integrazione consapevole di queste tecnologie nel contesto educativo, a seconda dell'utilizzo che ne fanno. La formazione include una comprensione approfondita delle tecniche per identificare e mitigare i *bias* nei contenuti generati dall'IA. La formazione si estende anche agli studenti per istruirli a un utilizzo responsabile dell'IA così da imparare a valutare criticamente i contenuti generati. L'obiettivo è dotare l'intera comunità scolastica di strumenti pratici e risorse utili per integrare l'IA in modo efficace e innovativo nelle attività quotidiane.
- **Integrazione di sistemi ibridi:** la definizione di un equilibrio tra l'utilizzo dell'IA e il contributo diretto del personale scolastico garantisce che l'aspetto umano rimanga centrale. I dirigenti scolastici, il personale amministrativo e gli insegnanti devono essere coinvolti attivamente nel monitoraggio delle attività, nell'adattamento delle risorse e nella gestione delle iniziative, anche quando queste sono supportate da strumenti automatizzati. Si suggerisce di integrare sistemi ibridi che automatizzino le attività ripetitive, lasciando spazio a interventi che preservino la relazione diretta con studenti e docenti. L'IA, infatti, non dovrebbe sostituire l'interazione umana e l'insegnamento diretto, ma arricchire le metodologie didattiche. Questo approccio combinato permette di promuovere un ambiente di apprendimento più inclusivo e coinvolgente.
- **Interazione sociale:** l'uso degli strumenti di IA deve essere alternato a momenti di apprendimento sociale, dove gli studenti possano interagire tra loro e con gli insegnanti. Attività collaborative, discussioni e lavori di gruppo possono contrastare l'isolamento, promuovendo il lavoro di squadra e le competenze interpersonali. Inoltre, per ostacolare una dipendenza eccessiva delle nuove tecnologie, gli studenti devono essere incoraggiati a utilizzare in maniera critica i sistemi dell'IA e renderli consapevoli dei benefici e dei potenziali pericoli. In questo modo potranno utilizzare e impiegare l'IA in modo etico e responsabile, eventualmente anche grazie al supporto di tecnici. L'obiettivo è assicurarsi che tali strumenti vengano usati a supporto e non a sostituzione delle decisioni o dei processi educativi.
- **Promozione del dialogo e del coinvolgimento:** una comunicazione chiara e trasparente permette di ottenere supporto e coinvolgimento da parte di tutti i soggetti interessati. Il personale scolastico dovrebbero avviare conversazioni in modo proattivo e invitare al dialogo, fornendo informazioni accurate e accessibili sull'integrazione dell'IA nelle scuole. Aggiornamenti regolari tramite newsletter e piattaforme digitali possono aiutare a diffondere informazioni e garantire trasparenza.

CONSAPEVOLEZZA E RESPONSABILITÀ NELL'UTILIZZO DELL'IA

L'introduzione di sistemi di IA deve avvenire nel rispetto dei principi in materia di etica, tenendo conto delle possibili implicazioni morali dei sistemi medesimi, al fine di supportare un uso corretto e antropocentrico dell'IA.

Studentesse e studenti devono essere guidati, tenuto conto del grado della scuola che frequentano, nel maturare una profonda consapevolezza delle potenzialità e dei limiti dell'IA ed essere supportati nello sviluppo di un adeguato senso critico che consenta loro di comprendere, analizzare e valutare le informazioni acquisite mediante i sistemi di IA, in modo autonomo e responsabile. A tal fine, fondamentale risulta il ruolo dei docenti nel fornire mezzi adeguati al potenziamento delle opportune competenze e abilità. Le competenze sviluppate da studentesse e studenti devono permettere loro di fruire in modo responsabile e corretto delle tecnologie emergenti, affinché possano sfruttare le relative opportunità e, al contempo, evitare utilizzi impropri delle stesse, a discapito dello sviluppo delle proprie conoscenze e abilità, con possibili ricadute negative sui relativi curricula e percorsi di crescita personale e scolastica.

Per lo svolgimento delle proprie funzioni educative e formative, è imprescindibile che i docenti siano costantemente aggiornati e acquisiscano gli strumenti necessari per un utilizzo sicuro, costruttivo e

funzionale dell'IA nel contesto scolastico.

Il dirigente scolastico, di concerto con le figure di riferimento da lui preposte, è chiamato ad effettuare un'attenta e delicata attività di verifica dei possibili sistemi di IA a cui poter ricorrere nello svolgimento delle attività didattiche, nella consapevolezza che l'utilizzo delle stesse per valutare i risultati dell'apprendimento, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento.

5. GESTIONE INFRASTRUTTURE E STRUMENTAZIONI

Tutte le persone (personale, esperti, studenti, genitori, visitatori, ecc) che portano nell'Istituto i device di loro proprietà sono responsabili del proprio dispositivo e lo portano nell'Istituto a proprio rischio.

Di conseguenza la scuola non è responsabile della sicurezza di tali dispositivi né deve farsi carico di eventuali risarcimenti.

INDICAZIONI GENERALI PER ACQUISIZIONE DI IMMAGINI E VIDEO DIGITALI

L'Istituto:

- chiede esplicito permesso del genitore/tutore legale per utilizzare fotografie digitali o video che coinvolgono il proprio figlio per produrre documenti interni alla scuola legati ad attività didattica. Questa autorizzazione viene sottoscritta all'atto dell'iscrizione.
- si impegna a richiedere un ulteriore permesso specifico alle famiglie per pubblicare materiali fotografici online o includere i nomi completi degli alunni nei titoli di qualsiasi materiale prodotto in documenti, video, ecc..

La scuola non risponde di eventuali foto o video pubblicate online dagli organi di stampa o da terzi senza che gli stessi abbiano chiesto autorizzazione ai genitori, né è responsabile di utilizzo improprio da parte degli utenti.

NORME PER GLI STUDENTI

L'uso dei device, proprio della scuola, segue il regolamento BYOD (*si veda a tal proposito l'allegato n. 19 al Regolamento d'istituto*), a cui si rimanda.

Telefoni e dispositivi elettronici non devono essere mai usati durante gli esami o prove nazionali e devono essere tenuti spenti. Questo porta alla esclusione dall'esame stesso e quindi all'immediata ripetizione dell'intero anno scolastico.

Situazioni possibili

Caso 1: Uso privato

In applicazione della normativa vigente (*DPR 249/1998; DPR 235/2007, DM 15.03.2007*) l'uso di device elettronici non è consentito per ricevere/effettuare chiamate o messaggi, giocare.

- Il divieto si applica anche negli intervalli e in tutti i momenti della giornata scolastica.
- Per quanto riguarda uscite, visite guidate e viaggi di istruzione, l'uso può essere consentito, se autorizzato dal docente, al di fuori dei momenti legati all'aspetto didattico dell'uscita.
- La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso la segreteria.
- La scuola chiede la collaborazione alle famiglie, nello spirito della corresponsabilità educativa,

evitando ad esempio di inviare messaggi o effettuare chiamate ai telefoni dei propri figli, durante l'orario scolastico o le visite di istruzione.

- Gli alunni sono tenuti a mantenere i loro device spenti durante l'intera permanenza a scuola, salvo quanto previsto nel caso di BYOD.
- Durante le attività didattiche non è consentito l'utilizzo di smartwatch e/o di qualsiasi altro dispositivo simile collegabile alla rete.

Caso 2: BYOD (Bring your own device-utilizzo per attività didattica)

Si veda l'allegato 19 al Regolamento d'istituto.

Caso 3: Dispositivo di proprietà del Liceo

- Il liceo mette a disposizione di chi ne avesse bisogno tablet e pc in comodato d'uso. I device sono disponibili sia durante l'anno che, eccezionalmente, nel periodo estivo previa autorizzazione.
- Gli insegnanti hanno la facoltà di decidere come e quando usare i dispositivi all'interno dell'istituto.
- La manutenzione e la responsabilità dei device sono a cura dello studente.
- Prima dell'atto della restituzione lo studente deve controllare che non siano stati salvati file e immagini personali, non potranno essere recuperati e la scuola declina ogni responsabilità per un utilizzo successivo alla data di restituzione del pc di tali file.

Tenendo conto delle indicazioni del Garante della privacy, si ribadisce che la registrazione delle lezioni è possibile solo per usi strettamente personali e, pertanto, previa autorizzazione di tutte le parti coinvolte.

La diffusione di tali contenuti è inoltre sempre subordinata al consenso da parte delle persone ritratte/riprese (minori e non; se minori l'autorizzazione va richiesta ai tutori legali/genitori) e della dirigenza della scuola.

Riprese audio/video o fotografiche effettuate e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni denigratorie, intimidatorie, vessatorie hanno carattere di reato penale.

NORME PER GLI ADULTI (tutto il personale scolastico, educatori, esperti esterni, ecc)

- L'uso del cellulare/tablet non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica, giocare, durante l'orario di docenza/lavoro.
- Il divieto si applica anche negli intervalli e nelle in altre situazioni che per responsabilità sono assimilabili ad attività didattica come cambio dell'ora e intervalli.
- Il personale non è autorizzato a utilizzare i propri telefoni cellulari o dispositivi a titolo professionale, come ad esempio per contattare gli alunni e/o le loro famiglie all'interno o al di fuori del proprio orario di lavoro e dall'Istituto.
- Il personale sui dispositivi dell'istituto non è autorizzato a consultare la e-mail personale (solo quella istituzionale) o ad accedere a siti e applicazioni per uso personale.
- Tutti i visitatori sono invitati a mantenere i loro telefoni e dispositivi personali sulla modalità silenzioso.
- Qualunque comunicazione dovrebbe essere in modalità nascosta o spenta. In ogni caso si deve evitare di essere raggiunti da qualsiasi notifica o segnalazione o eventi particolarmente distraenti e disturbanti la stessa attività didattica.
- Utilizzo del cellulare/tablet personale è ammesso per funzioni che possono avere rilevanza in ambito della propria professione e un possibile impiego nella didattica nello svolgimento delle lezioni. L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità didattica e professionale.
- Le riprese (fotografiche, vocali, video) potranno essere eseguite solo per scopi didattici dichiarati, con il consenso delle parti interessate (obbligatoria liberatoria dei genitori o tutori), e tenendo

conto delle indicazioni del Garante della privacy.

- RegISTRAZIONI o immagini effettuate durante lezioni, uscite didattiche o attività di presentazione allargate (come feste, eventi culturali, ecc...) possono essere utilizzate per usi esclusivamente didattici, di divulgazione delle attività dell'istituto e di documentazione pedagogica.
- Nessuno è autorizzato a pubblicare on line immagini di minori se essi sono riconoscibili.
- In caso di emergenza il personale della scuola (compresi educatori ed esperti di progetto), se non ha accesso immediato e semplice a un dispositivo di proprietà della scuola, è autorizzato ad utilizzare il proprio cellulare stando attento a non divulgare dati sensibili o personali.
- Il personale della scuola può utilizzare il proprio telefono cellulare seguendo le regole generali di non disturbo delle attività, in luogo non frequentato dagli studenti, se non in servizio.
- Se il personale è in attesa di una chiamata personale di urgenza chiede un'autorizzazione specifica per poter utilizzare il suo telefono al durante l'orario di lavoro, esclusivamente in modalità silenziosa.
- Se il personale viene a conoscenza di eventi di cyberbullismo, body shaming, discriminazioni di qualsiasi tipo online e/o su app sono obbligati a riferirlo alla famiglia e al Dirigente Scolastico.

INFRAZIONI E PROVVEDIMENTI

È assolutamente vietato:

Agli alunni

- usare la rete per giudicare, infastidire o impedire a qualcuno di esprimersi o di partecipare;
- inviare senza permesso foto o dati personali;
- condividere immagini intime o troppo spinte;
- comunicare incautamente con sconosciuti;
- collegarsi a siti web non indicati dai docenti durante le attività didattiche.

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

- il richiamo verbale;
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

Sono previsti anche interventi di carattere educativo:

- rinforzo dei comportamenti corretti;
- riparativi dei disagi causati con la partecipazione consapevole e attiva degli alunni;
- prevenzione e gestione positiva dei conflitti.

Al personale scolastico

- un utilizzo delle tecnologie non connesso alle attività di insegnamento o al profilo professionali;
- fornire la password del proprio registro personale ad altri;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisce un'adeguata protezione degli stessi;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- utilizzo a fini personali della strumentazione didattica;
- utilizzo non a scopo didattico dei device personali in orario di servizio.

UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DI INTERNET

Disposizioni sull'uso del laboratorio

- I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
- Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
- In caso di malfunzionamento o guasto dei computer bisogna darne segnalazione all'ufficio tecnico.
- Non lasciare alcun documento nel computer o nei dispositivi dell'istituto.

Disposizioni sull'uso dei software

- I software installati sono ad esclusivo uso didattico.
- È fatto divieto di usare software non conformi alle leggi sul copyright. Gli insegnanti possono fare installare software non free sui PC del laboratorio, informando il/la Dirigente.

Accesso a internet

- 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.
- È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.
- Il docente che verifica un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Accesso a internet: filtri, antivirus e navigazione

L'accesso a internet è possibile e consentito per la didattica nei laboratori multimediali o in classe tramite rete wireless solo dal computer del docente.

Sito web della scuola

La scuola attualmente ha un sito web all'indirizzo: www.liceoagnesi.edu.it

Tutti i contenuti del settore didattico sono pubblicati dopo averne valutato la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy.

Protezione dei dati personali

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).

6. E-MAIL ISTITUZIONALI

Da qualche anno sia ai docenti sia agli studenti è stato assegnato un indirizzo e-mail istituzionale, solitamente nella forma nome.cognome@liceoagnesi.edu.it

Le e-mail istituzionali sono attive e gestite dagli amministratori tramite Google Workspace for Education. L'utilizzo è esclusivo alla persona a cui viene assegnata.

Per motivi di privacy e sicurezza dei dati, per le comunicazioni interne all'istituto, ma anche quelle verso gli alunni e le famiglie devono avvenire tramite e-mail istituzionale o tramite registro elettronico. Anche l'accesso alle riunioni online sarà consentito solo utilizzando l'indirizzo e-mail istituzionale.

Associato all'indirizzo e-mail istituzionale è presente anche uno spazio drive personale che dovrà essere utilizzato per il salvataggio dei file personali e degli elaborati prodotti durante le lezioni, in modo di lasciare libero lo spazio sui dispositivi.

INDICAZIONI PER LA GESTIONE

In caso di smarrimento della password o di problemi nell'utilizzo presso l'ufficio tecnico si potrà trovare personale in grado di offrire assistenza.

7. PREVENZIONE

AZIONI

Le azioni previste di prevenzione nell'utilizzo delle TIC sono le seguenti:

- Informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire.
- Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a).
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola al di fuori dei contesti didattici autorizzati.
- Programmare percorsi di informazione e formazione da parte di esperti.
- Conoscere le sanzioni previste per chi utilizza in modo scorretto la rete e i dispositivi.
- Stabilire una *netiquette*, ovvero l'insieme delle norme di comportamento in rete.
- Inserire nel Patto di Corresponsabilità i comportamenti da rispettare.
- Aggiornare costantemente la pagina del sito dedicata a queste tematiche.

NB: Si parla di **bullismo** nel caso di comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti non da un solo soggetto, ma in genere da un gruppo. Si parla di **cyberbullismo** quando le azioni avvengono tramite la rete, ovvero:

- invio di sms, messaggi in chat, e-mail offensive o di minaccia;
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

Per quanto riguarda la prevenzione e il contrasto al **cyberbullismo** si rimanda alla **legge 71/2017**.

8. LINEE GUIDA

LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali;
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;
- Non inviare a nessuno fotografie tue o di tuoi amici;

- Prima di inviare o pubblicare la fotografia di qualcuno, chiedi sempre il permesso alla persona fotografata;
- Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
- Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
- Non rispondere alle offese ed agli insulti;
- Blocca i Bulli: molti siti e social network ti permettono di segnalare i cyberbulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere a tua volta accusato di cyberbullismo;
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
- Riferisci ai tuoi genitori (o al tuo insegnante) se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci ai tuoi genitori (al tuo insegnante) se ti capita di trovare immagini di questo tipo su Internet;
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo ai tuoi genitori (o al tuo insegnante);
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.

LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file sui computer o sul server della scuola, lo spazio è limitato e di uso comune, salvate i file nello spazio drive personale;
- Discutete con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informali che le navigazioni saranno monitorate;
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ridefinizione delle regole sociali di convivenza;
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi;
- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
- In caso di sospetto di abuso sessuale anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

- Far usare i dispositivi dei figli in vostra presenza;
- Evitate di lasciare le e-mail o file personali sui computer di uso comune;
- Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo...
- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;
- Aumentate il filtro del "parental control" attraverso la sezione sicurezza in internet dal pannello di controllo;
- Attivate il firewall (protezione contro malware) e antivirus;
- Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con

l'insegnante;

- Incoraggiate le attività on-line di alta qualità: ricercare informazioni;
- Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita agli estranei;
- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- Raccomandate di non scaricare file da siti sconosciuti;
- Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono messaggi indesiderati;
- Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;
- Il modo migliore per proteggere vostro figlio è usare Internet insieme, discutere e riconoscere i rischi potenziali.

9. DIDATTICA A DISTANZA

INFORMATIVA PER L'UTILIZZO DEGLI STRUMENTI FINALIZZATI ALL'EROGAZIONE DEL SERVIZIO DI DIDATTICA E FORMAZIONE A DISTANZA (DAD)

Premesso che a livello normativo la DAD è al momento prevista solamente per la didattica domiciliare, si specifica quanto segue:

Lo studente e la sua famiglia si impegnano a:

- a prendere visione dell'informativa predisposta all'uopo dall'Istituto, inviata tramite comunicazione alle famiglie del registro elettronico e consultabile anche sul sito internet della Scuola www.liceoagnesi.edu.it
- a rispettare il diritto alla disconnessione del docente, evitando di inviare comunicazioni di qualsiasi tipo in orari serali e durante il weekend, sottraendo così al docente il tempo necessario per ricaricarsi, per dedicarsi alla famiglia e alla propria vita personale;
- a conservare in sicurezza e mantenere segreta la password personale di accesso alla piattaforma di didattica a distanza, e a non consentirne l'uso ad altre persone;
- a comunicare immediatamente all'Istituto, attraverso e-mail indirizzata ai seguenti recapiti: lcps020004@istruzione.it PEC: lcps020004@pec.istruzione.it l'impossibilità ad accedere al proprio account del registro elettronico, il sospetto che altri possano accedervi, ed episodi come lo smarrimento o il furto della password;
- a non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma di didattica a distanza;
- a non diffondere eventuali informazioni riservate di cui si venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- ad osservare le presenti norme di comportamento, pena la sospensione da parte dell'Istituto dell'account personale dello studente e l'esclusione dalle attività di didattica a distanza e dai progetti correlati;
- ad utilizzare i servizi offerti solo ad uso esclusivo delle attività didattiche della Scuola;
- a non diffondere in rete le attività realizzate dal docente, con il docente e con i compagni;
- a non diffondere in rete screenshot o fotografie relative alle attività di didattica a distanza.
- quando ci si avvale di un PC in modo non esclusivo, non memorizzare la password ed effettuare sempre il logout.

NETIQUETTE PER LO STUDENTE

Ogni studente deve essere consapevole della necessità di rispettare le disposizioni previste dal *Regolamento UE 2016/679 (GDPR)*, così come adeguato e modificato con *D.LGS. n. 101 del 2018*.

Poiché il servizio è uno dei mezzi di comunicazione tra i docenti e lo studente, sarà dovere di ognuno accedere alla piattaforma impegnandosi a rispettare le seguenti regole:

- cercare, per quanto possibile, di inviare messaggi brevi che descrivano in modo chiaro l'oggetto della comunicazione; indicando sempre chiaramente l'oggetto in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto;
- utilizzare la piattaforma in modo da non danneggiare, molestare o insultare altre persone;
- non creare o trasmettere immagini, dati o materiali offensivi, volgari o sconvenienti;
- non creare o trasmettere materiale commerciale o pubblicitario;
- quando si condividono documenti, non interferire, danneggiare o distruggere il lavoro dei docenti o dei compagni;
- attivare la webcam solo nel momento in cui gli insegnanti chiedono espressamente di farlo;
- non registrare video o audio dei docenti senza il loro consenso (*Decreto Legislativo 196/2003, integrato con le modifiche introdotte dal D.lgs 101/2018*);
- non violare la riservatezza degli altri studenti, non ledere i loro diritti, la dignità e rispettare la loro privacy.

I docenti e l'Istituto non sono responsabili di eventuali danni arrecati allo studente a causa di guasti e/o malfunzionamenti del servizio ovvero per un non corretto utilizzo dello stesso e si impegnano affinché la piattaforma funzioni nel migliore dei modi. Lo studente e la sua famiglia si assumono la piena responsabilità di tutti i dati inoltrati, creati e gestiti attraverso la piattaforma di didattica a distanza.

F.to il Dirigente Scolastico

Dott.sa Sabrina Scola