



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

E-Safety Policy

INDICE DEI CONTENUTI

1. Introduzione

1. Scopo della *policy*.
2. Ruoli e responsabilità (*che cosa ci si aspetta da tutti gli attori della comunità scolastica*).
3. Condivisione e comunicazione della *policy* all'intera comunità scolastica.
4. Gestione delle infrazioni alla *policy*.
5. Integrazione della *policy* con Regolamenti esistenti.

2. Formazione e Curricolo

1. Curricolo sulle competenze digitali per la componente studentesca.
2. Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
Formazione del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

1. Accesso a internet: filtri, antivirus e sulla navigazione.
2. Gestione accessi (password, backup, ecc.).
3. E-mail.
4. Sito web della scuola.
5. Social network.
6. Protezione dei dati personali.

4. Strumentazione personale

1. Per la componente studentesca: gestione degli strumenti personali - cellulari, tablet ecc..
2. Per il corpo docente e per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi
- Azioni

Rilevazione

- Che cosa segnalare
- Come segnalare: con quali strumenti e a chi.
- Come gestire le segnalazioni.

Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso.



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

1. INTRODUZIONE

1.1 Scopo della *policy*.

Questa *policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.

In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica. Questo è il caso degli episodi di cyber-bullismo come di altri fenomeni di cui si tratta nella presente *policy*, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa.

L'IIS Curie-Levi accoglie studentesse e studenti "nativi digitali" che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

La scuola opera in stretto collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber-bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

1.2 Ruoli e responsabilità (*che cosa ci si aspetta da tutti gli attori della comunità scolastica*).

Dirigente Scolastico

È responsabile della presentazione di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti; deve anche valutare l'efficacia della politica e monitorarne/indirizzarne l'attuazione, anche in collaborazione con personale scolastico, enti locali e *stakeholder* territoriali. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.

Animatore digitale

Cura la redazione e la revisione annuale della *policy* sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola. Si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Personale docente, con particolare riferimento ai Coordinatori dei Consigli di Classe

Le insegnanti/gli insegnanti sono tenuti ad assicurare di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

- aver letto, compreso e sottoscritto la presente *policy*;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- integrare i problemi di sicurezza informatica in tutti gli aspetti del curriculum di studi e in altre attività extracurricolari;
- far comprendere e mettere in pratica alla componente studentesca le regole di comportamento relative alla sicurezza informatica;
- far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

Personale ATA

Il personale ATA è tenuto ad assicurare di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente *policy*;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;

Componente studentesca

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa *policy*. In particolare sono tenuti a:

- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali; capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.



Istituto di Istruzione Superiore “Marie Curie-Carlo Levi”

Sede “Marie Curie” - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata “Carlo Levi” - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS “Antonio Gramsci” - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso incontri con la Polizia municipale e altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di *e-safety* e a seguire le linee guida sull'uso appropriato di:

- immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli nella scuola (dove ciò sia consentito).

1.3 Condivisione e comunicazione della *policy* all'intera comunità scolastica.

Per evitare che l'adozione di questa *policy* rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:

Per il corpo docente, discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse della *policy*; un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla *policy* vigente; elaborazione di protocolli condivisi di intervento.

Per la componente studentesca, la discussione in classe della *policy* nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime e soffermandosi sui comportamenti da attuare in caso di bisogno.

Per i genitori, l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

1.4 Gestione delle infrazioni della *policy*.

Le infrazioni alla *policy* possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato che sia perseguibile d'ufficio, è fatto obbligo di denuncia (art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono, tra gli altri:

-*Minaccia*; in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 c. p.);

-*Induzione alla prostituzione minorile* (art. 600bis c. p.);

-*Pedopornografia* (art. 600ter c. p.);

-*Corruzione di minorenni* (art. 609quinq. c. p.).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si procede d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

Nel caso in cui le infrazioni della *policy* violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

1.5 Integrazione della *policy* con Regolamenti esistenti.

La presente *policy* è allegata in appendice al Regolamento di Istituto.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per la componente studentesca.

Le TIC e Internet sono un elemento essenziale nella vita del XXI secolo. La scuola ha il dovere di fornire alla componente studentesca l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale. L'uso consapevole delle TIC va inserito pertanto nel curricolo sia a livello disciplinare sia a livello interdisciplinare.

In particolare il curricolo dovrà essere strutturato per prevedere di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia per un pubblico più vasto;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare in modo critico le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

2.2 Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione potrà essere svolta da docenti dell'Istituto che fanno parte del team digitale ed è improntata alla condivisione di esperienze significative e di buone pratiche e all'occorrenza potrà vedere la partecipazione di esperti/consulenti esterni.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti dedicati di formazione presentati da enti e associazioni.



Istituto di Istruzione Superiore “Marie Curie-Carlo Levi”

Sede “Marie Curie” - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata “Carlo Levi” - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS “Antonio Gramsci” - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

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

3.1 Accesso a internet: filtri, antivirus e sulla navigazione.

L'Istituto ha configurato un *proxy server* per monitorare il traffico web. Nelle postazioni condivise sarà necessario prestare attenzione a non lasciare disponibili documenti contenenti informazioni personali e aver cura di non lasciare aperti e accessibili gli accessi ai propri profili di servizi basati sul cloud (a titolo di esempio non esaustivo: piattaforme di apprendimento, di condivisione file, account di posta elettronica, registro elettronico, ...). Andrà preferita, a tale riguardo, la modalità di navigazione anonima.

Attualmente le reti didattiche dei plessi Curie, Levi e Gramsci sono protette da sistemi hardware (Unifi UDM Pro) che integrano le funzionalità di firewall, proxy e controller wifi. È delegato a questi dispositivi il compito di *threat management*.

The screenshot displays the configuration interface for a Unifi UDM Pro device. The left sidebar shows 'Firewall & Security' settings, including Country Restriction (Off), Threat Management (Detect and Block), System Sensitivity (Medium), Dark Web Blocker (Enable), and Malicious Website Blocker (Enable). A red arrow points to the 'Edit threat categories' link. The main area shows 'Customize Threat Management (17 of 35)' with various threat categories and their status (checked/unchecked):

- Virus & Malware: Botnet (checked), Mobile Malware (checked), Worm (checked), Trojan (checked), Malware (checked)
- P2P: TOR (checked)
- Hacking: Exploit (checked), Shellcode (checked), DoS (unchecked), Attack Response (checked), Scan (checked), RPC (checked)
- Internet Traffic: Web Server (checked)
- IPs with a Bad Reputation: CI Army (checked), Compromised (checked), DShield (checked)

Si sconsiglia l'uso di antivirus sui computer o dispositivi usati dagli studenti in quanto eventuali malware sono bloccati a monte dall'UDM e quindi non penetrano da Internet; per tale motivo va disincentivato l'uso di chiavette o altri dispositivi di archiviazione personale di studenti e/o docenti che, in assenza di antivirus, bypasserebbero i sistemi di sicurezza perimetrali. Si ritiene che sia invece da incentivare l'archiviazione su cloud (drive scolastico o altri cloud personali) o su dischi di rete scolastici molto più facilmente gestibili.

Il filtro dei contenuti sensibili (materiali pornografici, violenza,...) al momento è delegato a un sistema esterno di gestione dei DNS (OpenDNS) che fornisce gratuitamente un sistema di *content filtering*. Anche se si potrebbe provvedere via UDM, c'è da dire che i sistemi proxy/content filter interni funzionano meno bene e sono molto più difficili da gestire da quando la maggior parte dei siti opera in protocollo https.

Si rammenta inoltre che il Google Workspace in uso fornisce intrinsecamente un servizio di rimozione del malware e di altre forme di minaccia (phishing, pharming, ...) altamente efficace.



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

3.2 Gestione accessi.

L'Istituto attualmente è dotato di una rete dedicata al solo utilizzo didattico da parte del corpo docente; la partecipazione ai progetti PNRR permetterà di estendere ulteriormente la strumentazione hardware/software, anche in un'ottica di didattica BYOD – *Bring Your Own Device*. Gli accessi alla rete sono gestiti tramite dei coupon personali usa-e-getta. Il recente PON reti cablate ha consentito di dare copertura wi-fi quasi totale ai locali della scuola con tecnologia di ultima generazione (Wi-Fi 6); pertanto il BYOD è già nella piena disponibilità dei docenti e degli studenti (è sufficiente richiedere un *voucher* che può essere configurato in termini di tempo e banda). Gli utenti che accedono al wi-fi scolastico attraverso un *voucher* sono isolati rispetto alle risorse della rete locale (pertanto non possono nuocere ad altri dispositivi).

L'Istituto intende mantenere un *log* corrente sull'uso dei sistemi della scuola per la verifica di eventuali violazioni della *policy*, oltre che delle leggi vigenti, da parte di chiunque abbia accesso a essi. La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

Si precisa che per quanto riguarda i *log*, al momento l'Istituto è in grado di tracciare l'indirizzo IP della macchina, il tipo di dispositivo, il tipo di traffico generato, ma non l'utente (mail personale o altro).

Si evidenzia comunque l'importanza di usare i dispositivi forniti dalla scuola solo per scopi scolastici e professionali, non a fini personali. Inoltre, occorre utilizzare i dispositivi in modo sicuro e rispettare le regole di utilizzo della scuola.

3.3 E-mail.

L'Istituto fornisce una casella di posta elettronica @iiscurielevi.it a tutto il personale docente/ATA e alla componente studentesca.

Gli account studenteschi hanno dei limiti che altri tipi di utenti (docenti, uffici, ..) non hanno: in particolare essi possono scrivere/ricevere, condividere/collaborare solo con il dominio scolastico (iiscurielevi.it) e pochi altri domini di fiducia gestiti a livello amministrativo. Gli account studente non possono avviare video-chiamate (possono ovviamente partecipare, ma solo se invitati). Per tutti le applicazioni di terze parti sono gestite a livello amministrativo.

Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo.

Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento, per consentire l'attivazione di protocolli di controllo.

E-mail in arrivo da mittenti sconosciuti o estranei al dominio vanno trattate come sospette ed eventuali allegati non devono essere aperti.

3.4 Sito web della scuola.

I dati di contatto sul sito web devono essere: indirizzo della scuola, e-mail e numero di telefono. Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5
assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

3.5 Social network.

La scuola è in grado di controllare l'accesso ai siti di social networking attraverso i *log* del *proxy server*; nel senso che è possibile tracciare quantitativamente le connessioni con i vari social. Nella pratica didattica si cerca di educare la componente studentesca al loro uso sicuro e consapevole. Per esempio, a ogni utente sarà consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione. Al momento non sussistono blocchi di navigazione sui social né si effettua il controllo individuale e sistematico sugli utenti che ne fanno uso, nell'ottica dell'educazione all'uso edotto e responsabile di cui sopra.

La componente studentesca non deve pubblicare senza espresso permesso scritto foto personali altrui su qualsiasi spazio di social network oppure che sia previsto nella piattaforma di apprendimento scolastico. Alunne/alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio.

Alunne e alunni saranno invitati a usare *nickname* e *avatar* non riconoscibili quando utilizzano siti di social networking.

La scuola non attiva chat o gruppi istituzionali su strumenti quali WhatsApp, Telegram e similari per la conversazione e condivisione non formale di informazioni tra utenti e non ne incoraggia l'uso; le comunicazioni che hanno valore ufficiale sono quelle pubblicate su canali istituzionali quali il sito web, la bacheca del registro elettronico, gli account ufficiali di profili Instagram, Facebook, ... Gli utenti pertanto sono invitati a servirsi dei canali formali.

3.6 Registro elettronico.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico è spiegato alle famiglie nel corso del primo consiglio di classe dell'anno scolastico e la pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a. Le credenziali sono strettamente personali e non vanno cedute a terzi.

Si rammenta al personale docente che occorre prestare massima attenzione a chiudere la propria sessione di accesso dopo l'utilizzo. Anche in tal caso, è preferibile attivare sessioni di navigazione in incognito.

3.7 Protezione dei dati personali.

Si fa riferimento a tutto quanto previsto dalla normativa comunitaria e nazionale vigente in fatto di riservatezza: GDPR (Regolamento Ue 2016/679). Tuttavia, si possono individuare al riguardo alcune linee guida di *e-safety*: in via generale il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori. Un telefono o una e-mail della scuola sarà fornito al personale esterno cui è richiesto il contatto con la componente studentesca o con i genitori.

Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.

I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, ... in particolare se in associazione con le loro fotografie.

All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati. Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento. Si ricorda che rispettare anche la privacy altrui rappresenta un obbligo di legge: non bisogna mai condividere informazioni personali di altri studenti, docenti o membri del personale senza il loro consenso scritto. Ciò include informazioni come indirizzi e-mail personali, numeri di telefono privati, immagini e altri dati sensibili.

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca.

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.

All'ingresso in aula, dopo l'appello, la componente studentesca deposita telefoni e altri dispositivi dentro un contenitore appositamente collocato in classe, la cui sorveglianza è in capo al corpo docente che si alterna durante le lezioni.

Individui con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia all'interno della classe.

Giochi e console portatili che possano avere accesso a Internet non filtrato non sono consentiti nemmeno se custoditi dentro i locali scolastici. Saranno requisiti dal docente che ravvisa l'infrazione, depositati nella cassaforte della segreteria e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

Occorre aggiornare regolarmente il software e le app per proteggere i dispositivi da eventuali vulnerabilità di sicurezza.

4.2 Per il personale docente/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5
all'interno di attività didattiche espressamente programmate.

I dati di accesso alla rete internet vanno custoditi con cura e per nessuna ragione vanno divulgati a chi non ha titolo per utilizzarla (genitori, operatori esterni, ...). L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili, ...) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe. Si demanda ai settori disciplinari la scelta dei settori su cui focalizzare la formazione: a titolo di esempio il dipartimento letterario si può soffermare in particolare sugli aspetti legati all'affettività, alla socializzazione e alla cittadinanza, quello tecnologico-scientifico-matematico sulle questioni tecniche e legate alla salute, quello di arte/diritto sulla tutela legale del diritto d'autore, ...

La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.

L'IIS Curie-Levi attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyber-bullismo e individua un docente interno referente per queste tematiche.

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

Le/gli insegnanti in particolare sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che le/gli adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni - quando non illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.



Istituto di Istruzione Superiore "Marie Curie-Carlo Levi"

Sede "Marie Curie" - Parco Gen. Dalla Chiesa, via Torino 9 - 10093 Collegno (TO) - tel. 0114046935

Sezione staccata "Carlo Levi" - via Madonna de la Salette 29 - 10146 Torino - tel. 011728351

Succursale c/o SMS "Antonio Gramsci" - via Giuseppe Di Vittorio 18 - 10093 Collegno (TO) - tel. 0114051220

email: TOIS067002@istruzione.it - PEC: TOIS067002@pec.istruzione.it - C. F. 95628490013 - Codice Univoco: UFDCU5

PREVENZIONE, RILEVAZIONE E GESTIONE

RISCHI	AZIONI
Adescamento online (<i>grooming</i>)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/social/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, <i>shopping</i> o <i>gambling</i> online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione dei minori e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curriculum di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità oltre che alla comunicazione non ostile. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
<i>Sexting</i> e pedopornografia.	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curriculum di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere cancellati mai più, né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

Delibera del Consiglio di Istituto n. 29 del 25 maggio 2023