REPUBBLICA ITALIANA

Buonarroti
Istituto Tecnico Tecnologico Trento

PROVINCIA AUTONOMA DI TRENTO

Regolamento per l'Uso degli Strumenti Elettronici e delle Piattaforme Digitali Scolastiche - DOCENTI & ATA

approvato in Collegio docenti il 26.03.2025
approvato in Consiglio dell'istituzione il 30.04.2025

Premessa

Il presente regolamento disciplina l'uso corretto e responsabile delle risorse informatiche, dei dispositivi elettronici e delle piattaforme digitali messe a disposizione della scuola per i docenti e il personale Ata e assistente educatore. L'obiettivo è garantire la sicurezza, la tutela della privacy e il rispetto delle normative vigenti, in conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR), il D.lgs. 196/2003 e le disposizioni del Garante per la Protezione dei Dati Personali. Esso costituisce parte integrante delle politiche di sicurezza dell'Istituto e vincola tutti i soggetti destinatari.

1 **Campo di Applicazione**

Il regolamento si applica a tutti i docenti e al personale scolastico che utilizza le risorse informatiche dell'Istituto, comprese le piattaforme digitali, i dispositivi elettronici e i servizi di comunicazione istituzionali. Sono altresì inclusi i dispositivi personali utilizzati per finalità scolastiche (BYOD), previa autorizzazione.

2 Utilizzo degli Strumenti Elettronici e delle Piattaforme Digitali

I dispositivi forniti dalla scuola devono essere utilizzati esclusivamente per attività didattiche o amministrative, in conformità con le finalità istituzionali dell'Istituto.

- **Software e Sicurezza**: È vietata l'installazione di software non autorizzato dall'amministratore di sistema o dal responsabile IT. Ogni dispositivo deve essere protetto da password complesse, aggiornate periodicamente, e sistemi di autenticazione a due fattori, ove disponibile.
- **Aggiornamenti**: È obbligatorio mantenere aggiornati il sistema operativo, il software antivirus e le applicazioni installate.
- **Utilizzo di Dispositivi Personali**: L'uso di dispositivi personali per la gestione di dati sensibili è consentito solo previa autorizzazione scritta del Dirigente Scolastico e previa verifica delle misure di sicurezza adottate. Inoltre, è obbligatorio adottare sistemi di controllo degli accessi e blocco del dispositivo quando non in uso, mantenendo i dati scolastici separati da quelli personali.
- **Privacy e Condivisione di Dati**: È vietato scattare foto o registrare video di studenti con dispositivi personali senza esplicito consenso scritto degli interessati o dei loro tutori legali. Utilizzare gli account creati e forniti dall'Istituto solo per lo svolgimento dell'attività professionale.
- **Archiviazione dei Dati**: Utilizzare come strumenti di archiviazione esclusivamente le piattaforme fornite dall'Istituzione scolastica. In caso di uso di dispositivi personali, evitare la memorizzazione di dati sensibili su unità esterne, che non siano espressamente autorizzate.
- **Piattaforme Didattiche**: Prima di utilizzare piattaforme didattiche diverse da quelle messe a disposizione dall'Istituto, che richiedano l'autenticazione, i docenti devono confrontarsi con il Dirigente Scolastico e il Responsabile della Protezione dei Dati (DPO), in quanto potrebbe essere necessaria l'autorizzazione delle famiglie.

3 **Trattamento dei Dati Personali**

I docenti sono tenuti a trattare i dati personali degli studenti in conformità al GDPR e al D.lgs. 196/2003, garantendo riservatezza, integrità e disponibilità dei dati.

- **Comunicazioni ufficiali**: Devono avvenire esclusivamente tramite canali istituzionali forniti dall'Istituto. È vietata la creazione di gruppi di messaggistica non istituzionali (es. WhatsApp) con studenti e genitori per motivi di sicurezza dei dati, tracciabilità e prevenzione di abusi.
- **Divulgazione di Dati Personali**: Non condividere informazioni personali degli alunni con colleghi o genitori di altri studenti se non strettamente necessario per motivi di lavoro. Mantenere rapporti professionali con i genitori attraverso i canali ufficiali.
- **Verifica dei Destinatari**: Verificare sempre attentamente i destinatari delle email per evitare divulgazioni errate di dati personali.

4 **Comunicazione e Collaborazione con Terzi**

- **Sicurezza dei Dati**: In caso di attività svolte in collaborazione con terzi, verificare che questi ultimi siano legittimati al trattamento dei dati degli studenti. Quando si inviano e-mail a più destinatari, utilizzare sempre il campo CCN per proteggere la privacy.
  A tal fine si ricorda:

CAMPO	SPIEGAZIONE
A	sono quelli dei destinatari PUBBLICI del messaggio
Cc	sono quelli di altre persone che vengono PUBBLICAMENTE informate dello scambio, pur non essendo i destinatari principali dello stesso;
Ccn	sono quelli di altre persone che vengono "SEGRETAMENTE" informate dello scambio, pur non essendo i destinatari principali dello stesso o quando abbiamo liste/elenchi di mail. In questo modo, tutti riceveranno la mail ma senza sapere a chi altri è stato inviato, mantenendo la riservatezza della comunicazione.

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Nello specifico:

- Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica.
- Ad ogni utente viene fornito un account e-mail nominativo nel dominio della scrivente. (buonarroti.tn.it), generalmente coerente con il modello **nome.cognome@buonarroti.tn.it;**
- L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato.
- L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa e di conservare e modificare frequentemente la password secondo le medesime indicazioni fornite per la gestione dell'account di accesso alle PdL.
- L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo "istituzionale" è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
- Allo scopo di garantire sicurezza alla rete della scrivente., evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità, con i quali non sussiste alcun rapporto

lavorativo o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js, *.xlse, *.xlsx e *.pif.

- È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing, frodi informatiche, od installazione involontaria di software malevolo. In qualunque situazione di incertezza, prima di eseguire qualsiasi azione, contattare gli amministratori di sistema per una valutazione dei singoli casi.
- Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile, anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietata la diffusione di messaggi pubblicitari di prodotti di qualsiasi tipo.
- Nel caso fosse necessario inviare allegati "pesanti" (oltre i 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalente. Nel caso di allegati ancora più voluminosi è necessario rivolgersi agli amministratori di sistema per la valutazione delle soluzioni. È necessario porre molta attenzione alla credibilità del messaggio di posta elettronica. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato
- Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati particolari e/o penali, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati crittati.
- Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.).
- È necessario configurare (o far configurare dall'AdS), un sistema di risponditore automatico da attivare in caso di prolungata assenza che avvisi il mittente della propria assenza.

- **Gestione della Documentazione**: Riporre documentazione contenente dati personali in armadi chiusi e custoditi. Garantire la sicurezza fisica degli uffici chiudendoli a chiave quando non presidiati.

5 Uso di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007. Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi:

a) È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dai sistemi di filtraggio implementati dall'Istituto o da Trentino Digitale s.p.a. con le sue policy di sicurezza, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner della scrivente, ecc.
b) È vietato compiere azioni che siano potenzialmente in grado di arrecare danno (sovraccarico della rete, introduzione di virus informatici), ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.
c) È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato.
d) Studio Gadler s.r.l. (DPO dell'ITT Buonarroti) si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento, e di predisporre filtri, basati

su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse, è possibile richiedere uno sblocco selettivo.

e) È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dallo Studio o comunque nell'ambito di un procedimento amministrativo che preveda dei movimenti finanziari.

f) È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet dalla propria postazione, utilizzando dispositivi personali se non espressamente autorizzati o per stretta necessità quando si sta lavorando all'esterno della struttura.

6 **Regolamento Comunicazione Digitale e Mastercom/registro elettronico**

- **Uso di Mastercom**: Mastercom deve essere utilizzato per la comunicazione alle famiglie e agli studenti riguardo a valutazioni, presenze/assenze, note disciplinari e altre informazioni didattiche. Inoltre, tramite Mastercom, genitori e studenti possono prenotare e svolgere a distanza le udienze con gli insegnanti e partecipare alle elezioni dei rappresentanti nei consigli di classe.
- **Canali Istituzionali**: La comunicazione con i genitori e con gli studenti deve avvenire esclusivamente tramite i canali istituzionali forniti dall'Istituto (mail e Mastercom), evitando l'uso di software di messaggistica istantanea (come WhatsApp) per comunicazioni istituzionali.

7 **Dispositivi Digitali Personali a Scuola**

- **Gestione dei Dispositivi Personali**: Qualora il dispositivo "ibrido" contenga dati o informazioni istituzionali qualificabili come personali, è obbligatorio seguire gli adempimenti previsti dal Regolamento Europeo e dai Provvedimenti dell'Autorità Garante. I dispositivi devono essere gestiti in modo da evitare la commistione tra i dati personali dell'utilizzatore e quelli dell'Istituto.
- **Sistemi di Sicurezza**: È necessario adottare meccanismi di identificazione e autenticazione, e mantenere i dispositivi protetti tramite password e blocco automatico quando non utilizzati. Si raccomanda di installare antivirus aggiornati e di verificare le licenze dei software installati.

PASSWORD
• Le **password** sono assolutamente personali e non vanno mai comunicate ad altri; • occorre cambiare immediatamente una password nel momento in cui diventa poco "sicura"; • le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri; • le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, post-it (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare); • le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password; • le password devono essere digitate in assenza di altri soggetti, i quali potrebbero vedere la tastiera, anche se collaboratori o dipendenti dell'azienda. In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Titolare.

DIVIETI
• Le **password** sono assolutamente personali e non vanno mai comunicate ad altri; • occorre cambiare immediatamente una password nel momento in cui diventa poco "sicura";

Per una corretta gestione delle password, l'organizzazione vieta di utilizzare come propria password:

a) nome, cognome e loro parti;
b) lo username assegnato;
c) un indirizzo di posta elettronica (e-mail);
d) parole comuni (in inglese e in italiano);
e) date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
f) parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
g) ripetizioni di sequenze di caratteri (es. abcabcabc);
h) una password già usata in precedenza.

8 Uso dell'Intelligenza Artificiale (AI)

8.1 Finalità e utilizzo consentito

Gli strumenti di IA possono essere utilizzati esclusivamente per scopi didattici autorizzati e nel rispetto delle linee guida stabilite dalla scuola. È vietato qualsiasi uso improprio che possa compromettere la privacy, l'integrità delle informazioni o violare le normative vigenti.

8.2 Uso consapevole ed etico

La scuola promuove un utilizzo responsabile ed etico dell'IA, sensibilizzando studenti e docenti sui I docenti sono chiamati a promuovere un utilizzo responsabile ed etico dell'IA, sensibilizzando gli studenti sui benefici e i rischi connessi a queste tecnologie. Ciò include l'organizzazione di attività formative specifiche per educare gli studenti a un uso consapevole e ponderato.

8.3 Tutela della privacy e sicurezza dei dati

I docenti sono tenuti a rispettare la normativa vigente e le disposizioni scolastiche per garantire la protezione dei dati personali degli studenti, la sicurezza del sistema informatico e la tutela della privacy, anche nell'uso di strumenti IA al di fuori dell'ambiente scolastico.

8.4 Limiti di età e responsabilità dei genitori

I docenti devono verificare che l'accesso degli studenti agli strumenti di IA avvenga nel rispetto dei limiti di età stabiliti dai fornitori. Al di fuori dell'ambiente scolastico, la responsabilità dell'uso di tali strumenti ricade sui genitori per i minorenni, mentre per i maggiorenni è a carico esclusivo dello studente.

8.5 Originalità e trasparenza nei contenuti generati con IA

I docenti devono assicurarsi che gli studenti non presentino come propri contenuti interamente generati dall'IA senza un'elaborazione personale. L'uso dell'IA nella produzione di materiali didattici deve essere dichiarato esplicitamente secondo le modalità concordate.

8.6 Responsabilità dei docenti

I docenti sono responsabili dell'uso corretto degli strumenti di IA nelle attività didattiche, nonché della supervisione dei materiali prodotti dagli studenti. Eventuali violazioni delle disposizioni potranno comportare sanzioni in conformità con il regolamento scolastico.

8.7 Divieto di utilizzi impropri

È vietato l'uso dell'IA per finalità non conformi al contesto educativo, inclusi utilizzi che possano favorire il plagio, diffondere informazioni fuorvianti o violare le politiche scolastiche e normative vigenti.

8.8 Responsabilità dell'Istituto e aggiornamento delle policy

L'Istituto si impegna a monitorare l'evoluzione delle normative e degli strumenti IA, aggiornando periodicamente le linee guida per garantire un utilizzo sicuro e conforme alla legge. I docenti sono tenuti a seguire gli aggiornamenti e a integrare le nuove indicazioni nelle loro pratiche didattiche.

9 **Regole per i docenti**

1. ***Utilizzo Responsabile***
   I docenti devono utilizzare gli strumenti IA esclusivamente per scopi didattici e formativi, rispettando le linee guida stabilite.
   È vietato l'uso dell'IA per attività non conformi alle regole scolastiche, come il plagio o la manipolazione delle risorse educative.
2. ***Consapevolezza***
   I docenti sono responsabili di educare gli studenti sui benefici e i rischi legati all'uso dell'IA, sviluppando capacità di analisi critica e consapevolezza sui limiti di tali strumenti.
   Devono guidare gli studenti nel comprendere che l'IA è uno strumento e non un sostituto del pensiero umano.
3. ***Protezione dei Dati Personali***
   I docenti sono tenuti a garantire che gli studenti non condividano informazioni personali sensibili tramite strumenti IA, a meno che non siano debitamente autorizzati e supervisionati.
   Devono informare gli studenti sui diritti relativi ai dati e sui meccanismi di protezione adottati dall'Istituto.
4. ***Dichiarazione d'uso***
   I docenti devono assicurarsi che l'uso dell'IA per la produzione di materiali didattici sia dichiarato esplicitamente con le modalità concordate.
   Sono responsabili della supervisione dei materiali prodotti dagli studenti, anche sotto il profilo disciplinare.
5. ***Responsabilità dei genitori***
   Resta ferma la responsabilità dei genitori per l'utilizzo degli strumenti di IA al di fuori dell'ambiente scolastico. I docenti devono sensibilizzare i genitori sull'importanza di monitorare l'uso degli strumenti IA da parte dei minorenni.

10 Uso dei Cellulari

10.1 **Uso durante le lezioni**

I telefoni cellulari e altri dispositivi personali (tablet, smartwatches, etc.) non devono essere utilizzati durante le lezioni, se non per motivi didattici espressamente autorizzati dal docente. È vietato l'uso di tali dispositivi per attività non legate alla didattica, inclusi giochi, social media, o comunicazioni non pertinenti.

10.2 **Dispositivi in modalità silenziosa**

Durante le lezioni tutti i dispositivi mobili devono essere tenuti in modalità silenziosa o spenti; **gli smartphone vengono riposti nell'apposita 'tasca' portacellulari a parete.** In caso di necessità urgenti, gli studenti e i docenti possono fare uso del dispositivo previa autorizzazione della direzione scolastica.

10.3 **Eccezioni**

L'uso dei telefoni cellulari è consentito esclusivamente per scopi educativi durante le attività in aula, come richiesto dal docente, o per attività didattiche specifiche che necessitano dell'uso di tecnologia.
Per il personale docente e ATA, l'uso di cellulari o altri dispositivi durante l'orario di servizio è permesso esclusivamente per motivi didattici o funzionali, come la consultazione del registro elettronico, la comunicazione con la segreteria o la direzione, o per la preparazione e spiegazione delle lezioni.

11 Responsabilità

11.1 Responsabilità degli studenti

Gli studenti sono responsabili dell'uso corretto dei dispositivi elettronici e delle piattaforme digitali, rispettando le regole e i principi definiti nel presente regolamento. Ogni violazione potrà comportare sanzioni disciplinari, come previsto dal regolamento interno della scuola.

11.2 Responsabilità dei docenti

I docenti sono responsabili del monitoraggio dell'uso dei dispositivi e delle piattaforme digitali durante le attività didattiche, assicurandosi che vengano rispettate le finalità educative e le norme relative alla privacy e alla sicurezza.

Il Dirigente Scolastico
(prof.ssa Tiziana Rossi)