IISS "Jacopo del Duca-Diego Bianca Amato" -
Cefalù
Via Pietragrossa, 68/70 -Telefono: 0921.421415
Cod. Fisc. 82000410827 – Sito internet: https://www.delduca-biancaamato.edu.it/
E-mail: pais02200v@istruzione.it - pais02200v@pec.istruzione.it

POLICY DI UTILIZZO DELLA STRUMENTAZIONE INFORMATICA

La presente Policy contiene la descrizione delle misure operative che i soggetti incaricati del trattamento dei dati personali sono chiamati ad adottare per garantire la sicurezza dei dati personali, in conformità agli standard di tutela previsti dal Reg. (UE) 2016/679 (GDPR).

Definizioni

Trattamento di dati: qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati (art. 5 GDPR).

Titolare del trattamento: persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione e organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel presente contesto, Titolare del trattamento risulta essere la Dirigente Scolastica Camilla Pasqualini in qualità di legale rappresentante dell'Istituto.

Responsabile del trattamento: persona fisica, giuridica, PA e qualsiasi altro ente, associazione, od organismo designati facoltativamente dal titolare al trattamento dei dati personali.

Incaricato del trattamento: chiunque agisca sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento (art. 29 GDPR).

Violazione dei dati personali (*): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, *12* GDPR)

Postazione di lavoro: Personal Computer, PC portatile, Tablet collegato alla rete informatica dell'Istituto tramite il quale l'utente accede ai servizi informatici.
Utente di posta elettronica: persona autorizzata ad accedere al servizio di posta elettronica.

Utente internet: persona autorizzata ad accedere al servizio Internet.
Log: archivio delle attività effettuate in rete dall'utente.

Internet Provider: azienda che fornisce alla scuola il canale d'accesso alla rete Internet.
Credenziali di autenticazione: codice utente e password richieste dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.

Art. 1 - Nomina del Custode delle password

Il Custode delle password è incaricato di custodire e conservare in luogo riservato e sicuro, in formato cartaceo, le credenziali. E' tenuto a ottemperare al suo compito avendo cura di non diffondere, nemmeno accidentalmente, le stesse a persone estranee al loro utilizzo.

Art.2- Assegnazione delle postazioni di lavoro

1. Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a:

- individuare preventivamente le postazioni di lavoro e assegnarle a ciascun dipendente,

- individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet.

2. La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere.

art. 3- Utilizzo delle password

1.Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dal soggetto nominato " Custode delle password". Le credenziali di autenticazione per l'accesso alla rete consistono in un codice per l'identificazione dell'utente (*user id*) associato ad una parola chiave (password) riservata che dovrà essere custodita dal Custode delle password con la massima diligenza e non può essere divulgata.

Art. 4- Procedure di gestione delle credenziali di autenticazione

1. È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Per scegliere una parola chiave si devono seguire le seguenti istruzioni (corroborate dal documento in allegato "ACN-GPDP Linee Guida Conservazione Password"):
-usare una combinazione di caratteri alfanumerici composta da almeno otto caratteri, di cui una lettera in maiuscolo e un carattere speciale, non facilmente intuibile;
-non usare mai il proprio nome o cognome, né quello di congiunti.

2. La password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il Custode della password (ogni sei mesi) e comunicata a quest'ultimo affinché ne curi la conservazione.
3. E' severamente vietato comunicare la propria password ad altri, trascriverla su supporti fisici (agenda, post-it, ...) che siano accessibili ad altri. Qualora l'incaricato del

trattamento abbia motivo di sospettare che la propria password sia stata letta , anche casualmente, da altri, essa deve essere immediatamente sostituita.

Art. 5- Utilizzo dei personal computer

1. Qualora al personale scolastico sia assegnato un personal computer di proprietà dell'Istituto, è fatto obbligo di :

- custodirlo con diligenza e in luogo protetto durante gli spostamenti;
  rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna;

- nell'ipotesi di lasciare incustodito il personal computer anche momentaneamente, effettuare il log-off dai diversi software gestionali, dispositivi informatici, o piattaforme software in uso, o quantomeno impostare uno screen-saver protetto da password;

- una volta superata la fase di autenticazione, non cedere l'uso del proprio dispositivo a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica;

- al termine di ogni sessione di lavoro, procedere allo spegnimento dei dispositivi informatici;

- consentire l'autoaggiornamento del PC;

- effettuare con cadenza regolare la cancellazione dei file obsoleti ed inutili dagli archivi.

2. Agli utenti dei personal computer non è consentito:

- installare programmi se non debitamente autorizzati;

- modificare le configurazioni esistenti;

- installare modem, router e switch o altri apparecchi se non debitamente autorizzati.

3. Ogni dispositivo di archiviazione di provenienza esterna all'Istituto dovrà essere verificato mediante programma antivirus prima del suo utilizzo.
Il Titolare del Trattamento o un suo delegato si riserva di effettuare controlli, conformi alla legge, anche saltuari e occasionali, per verificare la funzionalità e la sicurezza del sistema.

Art. 6 - Utilizzo dei personal computer/Tablet ad opera del Personale docente nell'ambito dell'attività didattica

1. Il personale docente è tenuto a guidare gli alunni e alunne nell'utilizzo dei personal computer/tablet dell'istituto scolastico nell'ambito dell'attività didattica, stabilendo obiettivi chiari per un uso consapevole di internet, e prevenendo il verificarsi di situazioni critiche tramite percorsi guidati funzionali all'arricchimento e all'ampliamento delle attività didattiche.

2. Ogni docente che utilizzi dispositivi informatici con i propri alunni/alunne, è tenuto a:

- illustrare ai propri allievi le regole di utilizzo;
- indicare siti appropriati per le ricerche ;
- monitorare la navigazione affinché alunni e alunne non accedano a siti non appropriati.

3. Qualora si riscontri un problema di funzionamento di un PC o di una LIM , il docente è tenuto a darne pronta segnalazione via e-mail al DSGA e al responsabile del laboratorio.

4. L'accesso alle postazioni informatiche è consentito agli alunni e alunne solo in orario scolastico e sotto la responsabilità del/della docente di riferimento.

5. L'accesso ai PC ed alla rete internet degli alunni/e deve avere una motivazione esclusivamente didattica.

6. L'uso di dispositivi di archiviazione di massa (chiavette USB e similari) deve essere limitato quanto più possibile - onde evitare immissione di virus nella rete scolastica - ed è sotto la diretta responsabilità del personale scolastico.

7. È vietato diffondere all'esterno la password di accesso alla rete Wi-Fi della scuola.

8. All'interno del perimetro scolastico non è consentito utilizzare /collegare dispositivi personali di condivisione della connessione Internet ("Web Cube" e similari).

9. In base alle vigenti norme sul diritto d'autore è vietato utilizzare le risorse della scuola per copiare/fotocopiare qualunque tipo di materiale protetto da copyright, ovvero duplicare CD e DVD protetti da copyright.

10. Internet non può essere usato per scopi vietati dalla legislazione vigente.

11. I residui di cibi e bevande possono danneggiare i computer e gli altri dispositivi (mouse, casse, etc.): è quindi vietato bere e mangiare in laboratorio o mentre si utilizzano gli strumenti.

12. E' vietato modificare la configurazione dei computer / tablet dell'Istituto scolastico (rete, desktop, ...).

Art. 7- Utilizzo di supporti magnetici

1. Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,...) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:

a) custodire i supporti magnetici in armadi o cassetti chiusi a chiave al fine di evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto, o reso conoscibile a terzi non autorizzati ;

b) consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili, ...) obsoleti al personale preposto per l'opportuna distruzione onde evitare che il loro contenuto possa essere recuperato successivamente alla cancellazione.

c) non rimuovere, danneggiare o asportare componenti hardware; qualora il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza.

Art. 8- Utilizzo delle stampanti e dei materiali d'uso

1. Stampanti e materiali di consumo in genere (carta, inchiostro, toner e supporti digitali) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi inopportuni.

2. Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e recarsi prontamente alla stampante comune per ritirare dai vassoi i fogli stampati, previo inserimento dei codici di accesso, evitando che le stampe restino incustodite e potenzialmente conoscibili da parte di soggetti non autorizzati.

3. Gli incaricati devono inoltre distruggere personalmente e regolarmente le stampe non più utili allo svolgimento delle mansioni.

Art. 9- Utilizzo di telefonini e altre apparecchiature

1. È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:

a) diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento;

b) informazione preventiva rivolta ai soggetti interessati;

c) acquisizione del libero e preventivo consenso dei soggetti interessati.

2. Gli utenti che utilizzano per il proprio lavoro computer/Tablet di proprietà dell'Istituto di cui sono responsabili, salvo eccezioni autorizzate dal datore di lavoro e dall'Amministratore di sistema, sono tenuti ad applicare al PC/Tablet portatile le regole di utilizzo previste per i PC connessi in rete.

Art. 10 - Sanzioni

In caso di abuso, a seconda della gravità del medesimo, fatte salve le ulteriori conseguenze di natura disciplinare, penale, civile e amministrativa, saranno messi in atto i seguenti interventi sanzionatori come da normativa vigente. Qualora l'abuso configuri gli estremi di un reato, si procederà a segnalare il fatto alle Autorità competenti. Il DSGA, in via provvisoria e di urgenza, e previa indicazione del Dirigente Scolastico (Titolare del Trattamento), può sospendere l'accesso dell'Utente senza preavviso, adottando le necessarie misure per impedire che l'abuso venga portato ad ulteriori conseguenze.

Il Dirigente Scolastico