Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per il Lazio
Ufficio Scolastico Provinciale di Roma

Liceo Scientifico "Amedeo Avogadro"

Via Brenta, 26 – 00198 Roma – ☎ 06121125905 - 🖷 068416085 www.liceoavogadro.gov.it
C.M.: RMPS030009, C.F.: 80202890580 , CUU eFatturaPA: UFI2PU

ALLEGATO 1

ISTRUZIONI OPERATIVE PER GLI INCARICATI DEL TRATTAMENTO

ISTRUZIONI OPERATIVE PER GLI INCARICATI DEL TRATTAMENTO

INDICE

INDICE 2

1 PREMESSA 3

2 RIFERIMENTI NORMATIVI E DEFINIZIONI 3

3 LINEE GUIDA 4

3.1 ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO 5
3.2 GESTIONE DELLE PASSWORD 6
3.3 ANTIVIRUS 6
3.4 SALVATAGGIO DEI DATI 7
3.5 SUPPORTI DI MEMORIZZAZIONE DEI DATI 8
3.6 PROTEZIONE DEI PC PORTATILI 8
3.7 INTERNET E POSTA ELETTRONICA 8
3.8 TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI 9
3.9 ARCHIVI CARTACEI 10

4 CONTROLLI DA PARTE DELLA TITOLARITA' 10

4.1 RIFERIMENTI NORMATIVI 10
4.2 ATTIVITÀ ISPETTIVA E PROCEDURE SANSONATORIE 11

5 SANZIONI CIVILI E PENALI 196/2003 11

ISTRUZIONI OPERATIVE PER GLI INCARICATI DEL TRATTAMENTO

1 PREMESSA

Il presente documento illustra le “linee guida” a cui gli **Incaricati del trattamento**, devono attenersi nel corso dello svolgimento delle proprie mansioni e in particolare nello svolgimento delle operazioni di trattamento di dati personali, in conformità a quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*" (di seguito Codice).

Si tratta di indicazioni da osservare scrupolosamente; pertanto, si consiglia agli Incaricati del trattamento di prestare la massima attenzione nella lettura delle disposizione di seguito enunciate.

Tale documento si applica, indistintamente, agli Incaricati "interni" che si trovano ad operare sui dati personali di cui il Liceo Scientifico “Amedeo Avogrado” è Titolare.

2 RIFERIMENTI NORMATIVI E DEFINIZIONI

Gli Incaricati sono le persone fisiche autorizzate a compiere le operazioni di trattamento dal titolare o dal responsabile (art. 4, comma 1, lettera h del Codice).
In particolare, ai sensi dell’art. 30, le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

La designazione è effettuata per iscritto e individua puntualmente l’ambito del trattamento consentito.

Si evidenzia preliminarmente che, ai fini del presente documento:

- con il termine “**trattamento**” (art. 4, comma 1, lett. a) ci si riferisce ad una qualunque operazione effettuata sui dati, svolta con o senza l'ausilio di mezzi automatizzati, che abbia come oggetto la raccolta, la registrazione, la consultazione, l’elaborazione, la modifica, la diffusione, l’estrazione, la distruzione di dati, anche se non registrati in una banca dati; il trattamento comprende l'intera vita del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine; di conseguenza, si parla di trattamento sia nel caso in cui vengano utilizzati mezzi elettronici o comunque automatizzati, sia altri mezzi che richiedono l'esclusivo apporto umano

- con il termine "**dato personale**" (art. 4, comma 1, lett. b) si fa riferimento a qualunque informazione relativa a persona fisica e giuridica, ente od associazione, siano esse informazioni nominative (come le generalità di una persona), o una qualunque altra informazione che possa rendere identificabile l'interessato, anche indirettamente (ad esempio codice fiscale, numero di matricola del dipendente)

- con il termine "**dato sensibile**" (art. 4, comma 1, lett. d) si fa riferimento ai dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato

- con il termine "**dato giudiziario**" (art. 4, comma 1, lett. e) si fa riferimento ai dati idonei a rivelare i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale.

3 LINEE GUIDA

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti assegnati, che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.
Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Incaricato deve osservare le seguenti regole di ordinaria diligenza nonché tutte le altre ed ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso, considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione; che ai dati possano accedere persone non autorizzate; che vengano svolte operazioni di trattamento non consentite o non conforme ai fini per i quali i dati stessi sono stati raccolti; che i dati non siano esatti o aggiornati
- in caso di allontanamento, anche temporaneo, dal posto di lavoro, si deve verificare che non vi sia possibilità da parte di terzi, anche se dipendenti, di accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato

- non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti
- si deve verificare l'esattezza e l'aggiornamento dei dati nonché la loro pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Si Sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà dell' Istituto Scolastico in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli dell' Istituto stesso.

Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

3.1 ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività
- utilizzata, laddove possibile, in modo esclusivo da un solo utente
- Ripulita, in caso di profili comuni, dei documenti, su cui si operava, al fine di evitare la diffusione impropria del dato trattato.
- protetta, in caso di abbandono momentaneo, richiamando le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL + ALT + CANC) ed assicurandosi della attivazione della funzione Lock Workstation o, in alternativa, impostando lo screen saver con password in modo che si attivi dopo 5/7 minuti di inattività.

Occorre, inoltre, precisare che spetta all'Incaricato:

- non utilizzare nel Liceo risorse informatiche private (PC, periferiche, token ecc..)
- non installare software la cui provenienza sia dubbia
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, ecc.)
- non lasciare, qualora ne foste dotati, il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione)

- non lasciare incustoditi, cellulari e palmari di proprietà del Liceo stesso
- non utilizzare fax, e-mail e/o telefono per trasmettere informazioni riservate qualora non si sia certi chela controparte è la persona incaricata a ricevere tali informazioni.
- non cestinare copie di documenti o appunti riservati senza averli prima distrutti

3.2 GESTIONE DELLE PASSWORD

Per una corretta gestione delle password, ciascun Incaricato deve aver cura di:

- modificare, alla prima connessione, la password che l'Area IT ha attribuito di default
- Comcambiare la password almeno ogni 90 giorni o immediatamente nei casi in cui sia compromessa
- comporre la password con almeno 8 caratteri alfanumerici, o nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito
- non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei familiari, la data di nascita, il codice fiscale
- mantenerla riservata e non divulgarla a terzi
- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente
- non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi
- non comunicare mai la password per telefono salvo gravi necessità.

3.3 ANTIVIRUS

I Personal Computer (PC) installati, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad attacchi di virus non conosciuti.

Per ridurre le probabilità di tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo
- chiudere correttamente i programmi in uso
- non aprire, se si lavora in rete, un file del quale si ha conoscenza di un comportamento sospetto

- non introdurre applicazioni/software che non siano state preventivamente approvate o la cui provenienza sia dubbia
- verificare con l'ausilio del programma antivirus in dotazione ogni supporto contenente dati (Pen-Driver o CD-Rom), prima dell'esecuzione dei file in esso contenuti
- non utilizzare CD-Rom o altri supporti elettronici di provenienza incerta
- non utilizzare supporti esterni già utilizzati su PC su cui è noto che si sono verificati malfunzionamenti
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet.
- non modificare le configurazioni impostate sul proprio PC
- spegnere il PC al termine della giornata di lavoro.

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'Incaricato:

- sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto
- contatti immediatamente l'Area IT o le figure addette
- chiuda il sistema e le relative applicazioni.

3.4 SALVATAGGIO DEI DATI

I dati vanno salvati sul server.

Al riguardo, qualora vi sia la necessità, l'Incaricato può richiedere all'Area IT la creazione sul server di una cartella a lui intestata o, in alternativa, di una cartella condivisa dal gruppo di lavoro cui fa riferimento l'Incaricato stesso (ad es. per gli Incaricati che gestiscono i dati dei dipendenti).

Qualora non sia presente un server centrale fare presente all'area IT o al personale addetto dell'esistenza di questi dati.

3.5 SUPPORTI DI MEMORIZZAZIONE DEI DATI

Nel caso in cui siano utilizzati supporti informatici quali cd-rom pen-Driver per la memorizzazione di dati sensibili e/o giudiziari, gli Incaricati devono osservare le seguenti misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i supporti informatici devono essere conservati in un luogo sicuro al fine di evitare accessi non autorizzati e trattamenti non consentiti
- i supporti informatici se non utilizzati devono essere distrutti o resi inutilizzabili
- i supporti informatici possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenute; l'operazione deve essere fatta in modo che i dati precedentemente memorizzati non siano tecnicamente ed in alcun modo recuperabili. Se l'operazione non è possibile è necessario distruggere i supporti.

3.6 PROTEZIONE DEI PC PORTATILI

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa.
Premesso che quanto indicato ai paragrafi precedenti è da adottarsi anche per i computer portatili vengono di seguito illustrate le ulteriori precauzioni cui ciascun utente è tenuto:

- conservare in un luogo sicuro l'elaboratore portatile a fine giornata lavorativa
- non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno del Liceo
- avvertire tempestivamente l'Area IT, che darà le opportune indicazioni, in caso di furto di un PC portatile
- essere consapevole delle informazioni archiviate sul portatile (il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa)
- operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti

3.7 INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati per le sole finalità di lavoro assicurando la massima diligenza. Sono vietati comportamenti che possono creare un danno al Liceo.

In particolare, occorre osservare le seguenti regole:

- navigare solo in siti attinenti allo svolgimento delle mansioni assegnate
- non scaricare software gratuiti (freeware) o shareware prelevati da siti Internet
- registrarsi solo nei siti i cui contenuti siano legati all'attività lavorativa
- partecipare solo per motivi professionali a Forum etc.
- non utilizzare funzioni instant messaging
- non aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro)
- non rispondere a messaggi provenienti da un mittente sconosciuto o con dubbio contenuto; spesso la risposta, in quanto tale, assicura al mittente l'esistenza del destinatario
- non utilizzare la posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione
- accertarsi sempre che i destinatari siano autorizzati ad entrare in possesso dei dati che stai inviando loro
- non accedere a siti Internet non correlati all'attività lavorativa e comunque non eticamente corretti
- tenere sempre a mente che la posta elettronica è un veicolo per l'introduzione sulla propria macchina (e quindi nel Liceo) di virus e altri strumenti potenzialmente dannosi.

3.8 TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

E' importante adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati.
A tal fine, onde evitare la diffusione di dati personali perseguibile civilmente e/o penalmente, ciascun Incaricato deve sempre avere cura di non lasciare in giacenza presso il fax, la stampante di rete o la macchina fotocopiatrice, documenti contenenti dati personali ed in particolare dati sensibili.

Essere certi che la controparte è la persona incaricata a ricevere tali informazioni.

3.9 ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Durante le normali quotidiane operazioni di lavoro, il materiale non dovrà risultare facilmente visibile a persone terze o comunque ai non autorizzati al trattamento.

In caso di trattamento di **dati sensibili e/o giudiziari**, tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento dalla postazione di lavoro.

Permettere l'accesso hai locali di lavoro solo a personale Incaricato dalla Titolarità.

4 CONTROLLI DA PARTE DELLA TITOLARITA'

Con il presente capitolo portiamo all'attenzione degli incaricati la possibilità di questo Istituto di effettuare controlli sulle proprie apparecchiature Tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

4.1 RIFERIMENTI NORMATIVI

- Linee guida del garante per posta elettronica e internet. Con questa delibera (Deliberazione n.13 del 1/03/2007 – pubblicata sulla G.U. n.58 del 10 marzo 2007) il garante pone particolare attenzione all'utilizzo dello strumento tecnologico di proprietà del azienda/istituto/ente/ etc. per usi personali da parte del dipendente. Sottolinea alle azienda/istituto/ente/ etc. la necessità di segnalare chiaramente ai propri dipendenti la possibilità da parte loro del controllo, da parte di appositi incaricati, degli strumenti tecnologici dati a loro in dotazione per l'espletamento dell' attività lavorativa. Tali controlli devono essere mirati alla preservazione della sicurezza dell' azienda/istituto/ente/ etc. stesso non a ledere i diritti di privacy del singolo. In conclusione l' azienda/istituto/ente/ etc. può controllare i propri strumenti tecnologici a condizione di aver avvertito i propri dipendenti di questa possibilità e avendo chiaramente indicato (come nei capitoli precedenti è stato fatto) che gli stessi possono essere utilizzati solo a fini Lavorativi.
- Tribunale di Torino, Sezione Distaccata di Chiasso, Sentenza 20 Giugno 2006 (dep. 15/07/2006), n.143. In questa Sentenza, ratificata anche dalla corte di cassazione, il giudice da il non luogo a procedere in quanto il fatto non sussiste. In poche parole Il PM voleva condannare la Ditta XXX per aver effettuato un accesso presso la postazione informatica della propria dipendente senza il consenso della stessa. Grazie al documento interno della ditta in cui si sottolineava che lo strumento informatico era di proprietà della stessa e che potevano quindi regolarmente accedervi. Il Giudice ha dato il non luogo a procedere.

4.2 ATTIVITÀ ISPETTIVA E PROCEDURE DISCIPLINARI

- Questo Liceo nel corso degli anni si è dotato di strumenti tecnologici al fine di migliorare la produttività e la sicurezza del Liceo stesso. Il personale Tecnico che compie attività di manutenzione Hardware e Software ha ricevuto specifiche indicazioni per il comportamento deontologico che devono adottare nella ordinaria e straordinaria manutenzione a fine di tutelare i dati.
- Se nelle normali attività manutentive si dovessi rilevare un uso improprio della strumentazione elettronica il personale Tecnico sarà tenuto ad informare la titolarità di quanto rilevato.
- In caso utilizzo improprio da parte del dipendente dello strumento informatico/tecnologico la titolarità potrà procedere con misure disciplinari commisurate alla natura dell'infrazione.

5 SANZIONI CIVILI E PENALI

Riferimento alla Normativa 196/2003

"La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore."

"Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi"

Redatto da	**Marco Casati** (Sicurezza informatica e Privacy)	
Responsabile del documento	**Valter Auddino** (Responsabile Privacy)	
Approvato ed Emanato da	**Prof.ssa Stefania Senni** (Titolare Privacy)	

Ultima pagina del documento