Ministero dell'Istruzione dell'Università e della Ricerca
ISTITUTO TECNICO COMMERCIALE STATALE "ABBA - BALLINI"
Via Tirandi n. 3 - 25128 BRESCIA
tel. 030/307332-393363 - fax 030/303379
bstd15000l@pec.istruzione.it www.abba-ballini.gov.it email: info@abba-ballini.gov.it

Ulteriori istruzioni per gli Incaricati del trattamento dei dati. Unità organizzativa: FIGURE PREVISTE DAL D.lgs 81/2008

Ciascun incaricato del trattamento dei dati deve attenersi scrupolosamente alle seguenti istruzioni:

1. essere consapevole del fatto che, nell'espletamento delle proprie funzioni, può venire a conoscenza di dati personali e/o di dati sensibili riguardanti il personale, gli alunni e i loro familiari. In questi casi, s'impegna ad operare con serietà, correttezza e scrupolo, affinché detti dati siano gestiti in maniera corretta e riservata, in ottemperanza con quanto prescritto dal D.Lgs. 196/2003 e da successive modifiche e integrazioni, e non siano divulgati o comunicati, in tutto o in parte, a persone e/o ad organizzazioni senza che ve ne sia una reale necessità giustificata da comprovate e motivate esigenze e comunque sempre nel rispetto delle leggi e del regolamento predisposto dal M.P.I. ;
2. impegnarsi a non soddisfare richieste di conoscenza o accesso ai dati personali o ai dati sensibili, nel caso in cui non sia chiara ed evidente la liceità delle richieste stesse e nel caso in cui le richieste siano formulate tramite telefono o posta elettronica. In questi casi informare il DSGA o il Dirigente Scolastico;
3. essere consapevole che le risorse informatiche e telefoniche sono di proprietà della scuola e che devono essere utilizzate per fini strettamente lavorativi e assolutamente non per scopi diversi né tanto meno per fini personali. Anche la casella di posta ed il collegamento ad Internet devono essere considerati strumenti di lavoro, per cui le persone assegnatarie devono ritenersi responsabili del corretto utilizzo degli stessi e devono essere consapevoli che il Dirigente Scolastico può svolgere dei controlli, anche su richiesta del Responsabile del trattamento dei dati;
4. per i trattamenti dati su supporti cartacei seguire le linee guida qui di seguito elencate:
   A) **I dati su supporti cartacei in genere**, (verbali, relazioni, ecc) devono esser gestiti con cura, non devono rimanere incustoditi soprattutto se contenenti dati sensibili e/o giudiziari. Al termine del loro utilizzo o comunque al termine della giornata lavorativa, devono essere riposti in un luogo chiuso e sicuro; se trattasi di dati di tipo sensibile e/o giudiziario vanno chiusi a chiave in armadi o cassetti o contenitori dotati di serratura e di chiave funzionante. Quando non più necessari, i documenti cartacei devono essere restituiti o distrutti.
   B) **Nella compilazione di relazioni, verbali ecc**, l'inserimento dei dati sensibili e/o giudiziari deve avvenire solo quando è indispensabile. In questi casi rendere anonimi i dati (se la cosa non impedisce la fruibilità del documento da parte di chi è autorizzato a vederlo) attraverso la codifica del nominativo della persona oggetto del trattamento.

per i trattamenti dati su supporti elettronici seguire le linee guida qui di seguito elencate:

C) **PASSWORD:** le proprie password devono essere composte minimo da 8 caratteri alfanumerici, con numeri e lettere, di cui almeno una maiuscola. Devono essere custodite scrupolosamente e non devono essere comunicate ad altre persone.

D) **VALIDITÀ PASSWORD:** la password per l'accesso alla rete amministrativa (nel caso si sia autorizzati all'accesso), o didattica (quando vi è un domino e si rientra negli utenti accreditati), ai vari programmi applicativi e a tutti i software che ne prevedono l'uso per l'accesso, devono essere sostituite almeno ogni sei mesi. **Per i dati sensibili la password deve essere sostituita ogni tre mesi**.

E) **PROTEZIONE DOCUMENTI ELETTRONICI CONTENTI DATI SENSIBILI E/O GIUDIZIARI:** nei casi in cui si producano documenti contenenti tali tipi di dati si provvederà alla loro conservazione in cartelle a specifico accesso, riservate in lettura e modifica ai soli autorizzati al trattamento.

F) **SALVATAGGIO DEI DOCUMENTI:** tutti i documenti realizzati con l'ausilio del PC devono di norma esser salvati nella propria cartella sul Server quando è disponibile.
Negli altri casi i dati possono essere salvati su supporti removibili (quali cd-rom, dvd, supporti USB), ma si fa presente che la protezione dei documenti su tali supporti è a carico di chi li ha prodotti. Per i dati che eventualmente vengono salvati sul disco fisso dei PC, la scuola non può in alcun modo essere considerata responsabile in caso di intrusioni, danneggiamenti, perdite o altro. Per tali dati (quelli salvati su PC in locale) ciascuno è responsabile del salvataggio, con frequenza almeno settimanale (così come previsto dall'art. 18 del Disciplinare Tecnico).

G) **CANCELLAZIONE DATI DA SUPPORTI REMOVIBILI:** quando un'intera serie di dati contenuti su cd-rom, dvd, USB ecc. devono essere eliminati, si deve formattare il supporto stesso in quanto non è sufficiente la semplice cancellazione dei dati. Per quanto invece concerne i cd-rom che non sono più necessari, non potendo esser cancellati in alcun modo, devono esser fisicamente distrutti mediante frattura del cd stesso.

H) **SOFTWARE ANTIVIRUS:** il software antivirus installato sul PC non deve mai e per nessun motivo essere disabilitato in quanto, in tal caso, il PC non è più protetto da eventuali attacchi da virus, compromettendo così la sicurezza dell'intera rete. É necessario quindi verificare che vicino all'orologio della barra di avvio di Windows (posizione standard: basso a destra nel monitor) sia sempre presente l'icona dell'antivirus.

I) **VIRUS E POSTA ELETTRONICA:** a coloro che utilizzano la posta elettronica a scuola si raccomanda di porre sempre attenzione al tipo di file allegati ai messaggi ricevuti, anche se il software antivirus è presente e abilitato. É necessario quindi diffidare dei file allegati con estensione del nome tipo EXE, COM, VBS, PIF, BAT e di tutti quelli che presentano una doppia "falsa" estensione (come ad esempio "VIDEO.AVI.VBS").
Queste tipologie di file sono infatti, in molti casi, i veicoli per la diffusione di virus.

Spesso questi file sono inviati racchiusi in un archivio zippato; prima di estrarre qualsiasi documento verificare che i file contenuti non abbiano le estensioni prima descritte. Si raccomanda, nel caso in cui si ricevono messaggi con questo tipo di allegati, di avvisare l'amministratore di sistema prima di aprirli, anche se la fonte da cui proviene il messaggio è più che attendibile.

J) **INTERNET:** richiamando quanto indicato nel punto 3, si ricorda che il collegamento a Internet deve essere considerato come uno strumento di lavoro e deve essere utilizzato correttamente ed in modo responsabile.
Il Responsabile del trattamento dei dati e il Dirigente Scolastico, eventualmente tramite l'Amministratore di Sistema, si riservano i diritti di poter compiere dei controlli per verificarne l'uso corretto e di intervenire nei casi di utilizzo irregolare.

K) **INSTALLAZIONE DI SOFTWARE:** ogni software che l'utente ha bisogno di installare sulla propria postazione o su le postazioni dei laboratori, in quanto strettamente necessario all'espletamento delle proprie funzioni, deve essere richiesto al Responsabile del laboratorio o al Dirigente, il quale chiederà all'Amministratore di Sistema di sottoporlo ad una verifica di compatibilità software/hardware. Si rammenta che non possono in alcun modo esser caricati, su PC di proprietà della scuola, programmi che non sono stati regolarmente acquistati e dotati di regolare licenza d'uso, nonché esplicitamente autorizzati dal Dirigente. Nel caso non venisse osservata la presente norma, l'istituzione scolastica si riserva il diritto di richiedere, a titolo di risarcimento danni, le somme pagate a fronte di multe o sanzioni amministrative comminate da parte della Guardia di Finanza, del Garante per la protezione dei dati, della Polizia Postale o di altre organizzazioni autorizzate, nonché, nel caso in cui il programma non autorizzato abbia causato un malfunzionamento del PC, le somme pagate a ditte esterne o il corrispondente economico delle ore impiegate per rimetterlo in funzione.

L) **ASSENZA PROLUNGATA DAL POSTO DI LAVORO:** nel caso in cui un utente si debba allontanare dalla propria postazione, è tenuto alla disconnessione del proprio elaboratore dalla rete, in modo che il successivo accesso richieda nuovamente utente e password. Inoltre è possibile e consigliato inserire nella propria postazione la protezione da password temporizzata (ad esempio dopo 5 minuti di inattività) tramite le impostazioni dello screen saver.

IL DIRIGENTE SCOLASTICO

(Elena Lazzari)